PHYSICAL LAYER SECURITY TECHNIQUES FOR FUTURE WIRELESS COMMUNICATION SYSTEMS AGAINST EAVESDROPPING

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

Haji M. Furqan Ahmed Madni

August, 2020

Physical Layer Security Techniques for Future Wireless Communication Systems Against Eavesdropping
By Haji M. Furqan Ahmed Madni
August, 2020

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

Prof. Dr. Hüseyin Arslan(Advisor)

Prof. Dr. Mesut Kartal

Prof. Dr. Bahadır Kürşat Güntürk

Assoc. Prof. Dr. Ertuğrul Başar

Assist. Prof. Dr. Tunçer Baykaş

Approved by the Graduate School of Engineering and Natural Sciences:

Assoc. Prof. Dr. Yasemin Yüksel Durmaz
Director of the Graduate School of Engineering and Natural Sciences

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: HAJI M. FURQAN AHMED MADNI

Signature :

ABSTRACT

PHYSICAL LAYER SECURITY TECHNIQUES FOR FUTURE WIRELESS COMMUNICATION SYSTEMS AGAINST EAVESDROPPING

Haji M. Furqan Ahmed Madni
Ph.D. in Electrical, Electronics Engineering and Cyber Systems
Advisor: Prof. Dr. Hüseyin Arslan
August, 2020

The inherent broadcast characteristics of wireless communication make it vulnerable to passive eavesdropping. Conventionally, security techniques in the upper layers like cryptography-based techniques have been employed for secure transmission. However, such security techniques may not be adequate for future decentralized networks due to their high complexity of implementation and computation. Furthermore, the emergence of powerful computing devices makes these techniques vulnerable to sophisticated adversaries. To cope up with these problems, physical layer security (PLS) techniques have attracted a lot of attention. PLS techniques exploit the dynamic features of wireless communications, for example, the randomness of the channel, interference, and noise, etc., to restrict the eavesdropper from decoding the data while ensuring the successful decoding of data for the legitimate user. In this thesis, novel security techniques are proposed and developed based on the physical layer of wireless communication to provide secure communication against eavesdropper. The main approaches in the conducted research include the security techniques for the applications in the following domains: multiple-input-multiple-output (MIMO), cooperative communication, orthogonal frequency division multiplexing (OFDM), orthogonal frequency division multiplexing with index modulation (OFDM-IM), cognitive radio (CR), non-orthogonal multiple access (NOMA), and heterogeneous networks. Moreover, an intelligent framework for physical layer security is also presented.

Keywords: Security, Physical layer security, OFDM, 5G, PHY.

ÖZET

GELECEKTEKİ KABLOSUZ İLETİŞİM SİSTEMLERİ İÇİN GİZLİ DİNLEMEYE KARŞI FİZİKSEL KATMAN GÜVENLİK TEKNİKLERİ

Haji M. Furqan Ahmed Madni
Elektrik-Elektronik Mühendisliği ve Siber Sistemler, Doktora
Tez Danışmanı: Prof. Dr. Hüseyin Arslan (Advisor)
Ağustos, 2020

Kablosuz iletişimin doğasında bulunan yayılım özellikleri, onu pasif dinlemeye karşı savunmasız kılmaktadır. Geleneksel olarak, güvenli bir iletim için üst katmanlarda kriptografiye dayalı güvenlik teknikleri kullanılmıştır. Bununla birlikte, bu tür güvenlik teknikleri, yüksek uygulama ve hesaplama karmaşıklıkları nedeniyle gelecekteki merkezi olmayan ağlar için yeterli olmayabilmektedir. Ayrıca, güçlü bilgi işlem cihazlarının ortaya çıkışı, bu teknikleri ileri teknolojiye dayalı rakiplere karşı savunmasız hale getirir. Bu sorunların üstesinden gelmek için, Fiziksel Katman Güvenliği (PLS) teknikleri büyük ilgi görmüştür. PLS teknikleri, meşru kullanıcı için verilerin başarılı bir şekilde çözülmesini sağlarken, gizli dinleyicinin verilerin kodunu çözmesini kısıtlamak için, kanalın rasgeleliği, girişim ve gürültü gibi dinamik özelliklerinden yararlanır. Bu tezde, dinleyicilere karşı güvenli iletişim sağlamak için kablosuz iletişimin fiziksel katmanına dayalı olarak yeni güvenlik teknikleri önerilmiş ve geliştirilmiştir. Yürütülen araştırmadaki ana yaklaşımlar, aşağıdaki alanlardaki uygulamalar için güvenlik tekniklerini içermektedir: Çoklu-giriş çoklu-çıkış (MIMO), işbirliğine dayalı iletişim, Dikey Frekans Bölmeli Çoklama (OFDM), İndeks Modülasyonlu Dikey Frekans Bölmeli Çoklama (OFDM-IM), Bilişsel Radyo (CR), Dikey Olmayan Çoklu Erişim (NOMA) ve heterojen ağlar. Ayrıca, fiziksel katman güvenliği için akıllı bir çerçeve de sunulmaktadır.

Anahtar sözcükler: Güvenlik, Fiziksel katman güvenliği, OFDM, 5G, PHY.

Acknowledgement

First, I extend my gratitude and thanks to Allah and RasulAllah (peace be upon him) for everything. I would like to thank my respected advisor Prof. Dr. Hüseyin Arslan for his support, motivation, and guidance throughout my studies. I would also like to express my thanks to Assist. Prof. Dr. Tunçer Baykaş, Prof. Dr. Bahadır Kürşat Güntürk, Assoc. Prof. Dr. Ertuğrul Başar, and Prof. Dr. Mesut Kartal for serving in my committee and offering constructive comments.

I would like to thank all my friends in both CoSiNC group and WCSP group for their faithful bits of advice and productive discussions as colleagues. And specially those, who supported me in every chapter of my life.

Last, but not least, I would like to offer my gratitude to my parents, my brothers, and my sisters for their continuous and unconditional love and support during these years.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Fifth-generation (5G) wireless systems are not just simple evolution of conventional fourth-generation (4G) networks, but they are also expected to offer many new services beyond internet to critical communication and internet of things (IoT). The three main services of 5G include ultra-reliable low latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC) [7]. Overall, 5G will have a significant impact on many areas of life [8] [9] and will bring a lot of interesting applications such as autonomous driving, virtual reality, smart city, smart energy networks, remote surgery, drone delivery, and so on. However, due to the broadcast nature of wireless communication, 5G is vulnerable to eavesdropping, which may compromise the confidentiality of the signals.

The conventional solutions to provide secure communication in wireless technologies are based on cryptography, but they may not be well-suited for future communication [10] due to the following reasons: firstly, future networks consist of decentralized and heterogeneous wireless networks in which key management processes are quite challenging. Secondly, future networks need to support

new wireless technologies such as the IoT including both mMTC and URLLC. The transceiver devices in these wireless technologies are naturally power-limited, processing-restricted, and delay-sensitive which make cryptography-based techniques infeasible for such types of technologies. Thirdly, future networks are expected to support diverse services and scenarios that have different levels of security requirements. However, encryption-based methods can only provide a binary level of security [10]. To cope up with these problems, PLS techniques have emerged as a promising solution that can complement and may even replace the cryptography-based approaches [11]. PLS exploits the dynamic features of wireless communications, for example, random channel, fading, interference, and noise, etc., to prevent the eavesdropper from decoding data while ensuring that the legitimate user can decode it successfully [10]. PLS has the following advantages with respect to future networks as compared to cryptography. Firstly, PLS approaches can be exploited to extract keys from the channel that is common between legitimate transmitter and receiver, thus avoiding key management issues. Secondly, some of the PLS approaches can be implemented by relatively simple signal processing techniques which make it suitable for processing-restricted and delay-sensitive services. Thirdly, in PLS, channel-dependent resource allocation and link adaptation can be designed to provide flexible and scenario-specific security schemes [11].

The advantages and significance of PLS motivate us to design and develop new practical security techniques by exploiting the intrinsic properties of the wireless channel. In this thesis, new and effective security techniques are proposed for current and future wireless communication systems by exploiting and redesigning some significant enabling technologies such as multi-antenna transmission, multi-carrier waveforms, and cooperative communication, cognitive radio, etc. The proposed security techniques ensure secure communication against eavesdropper by exploiting the dynamic physical properties of the wireless channel such as noise, interference, and fading, etc.

1.2 Scope of the Thesis

The scope of this thesis is to develop and design novel techniques to provide secure communication against eavesdropping by exploiting the functionalities of the physical layer in wireless communication systems. The chapters contain the details about the related literature review, considered system model, proposed security algorithms, and their performance evaluation through simulation results.

More specifically, the conducted research covers the following main directions: a) **security technique for multiple-input and multiple-output (MIMO) systems** such as secret key generation using channel quantization with singular value decomposition (SVD) for reciprocal MIMO channels, b) **security techniques for multi-carrier communication** such as a new physical layer key generation dimension: indices based key generation, enhancing PLS of OFDM-based systems using channel shortening, adaptive OFDM-IM for enhancing PLS & spectral efficiency, and secure and reliable IoT communications using non-orthogonal signals' superposition with dual-transmission, c) **techniques related to cooperative communication** such as secure communication via untrusted switchable decode-and-forward relay, d) NOMA related such as PLS for NOMA: requirements, merits, challenges, and recommendations, e) Works related to physical layer authentication such as Primary User Emulation and Jamming Attack Detection in Cognitive Radio via Sparse Coding, f) work related to intelligent physical layer security such as cognitive security of wireless communication systems in the physical layer.

1.3 Thesis Contributions

The main contributions of this research related to physical layer security include following main topics

- **Physical Layer Security Designs for 5G and Beyond**

Physical layer security (PLS) has emerged as a promising and powerful concept for securing future wireless technologies, including fifth generation (5G) and beyond networks, as it has the potential to solve many of the problems associated with conventional cryptography-based approaches. In this chapter, the principles of PLS as a complementary solution to cryptography for future networks are presented. The concepts, merits, and demerits for different types of PLS techniques are discussed and explained. Moreover, the recent applications of PLS to different emerging wireless technologies are also presented. Furthermore, the details about physical layer authentication methods against spoofing attacks and details about jamming attacks and related solutions are also included.

- **Secret Key Generation Using Channel Quantization with SVD for Reciprocal MIMO Channels**

  The generation of secret keys from reciprocal wireless channel by exploiting their randomness nature, is an emerging area of interest to provide secure communication. One of the main challenges in this domain is to increase the secret key length, extracted from the shared channel coefficients between two legitimate communication parties, while maintaining its randomness and uniformity. In this work, we develop a practical key generation method, based on channel quantization with singular value decomposition (CQSVD), which is capable of significantly increasing the generated secret key in MIMO systems. This is achieved through quantizing the phases and amplitudes of the estimated MIMO channel coefficient's matrix by using an alternative form of SVD, where the key sequence is extracted from the orthogonal basis functions of the decomposed channel. The extracted key sequence is transformed to a random phase sequence, which is then used to manipulate the transmitted data on a symbol level basis rather than bit level-basis, to provide more secure communication. The comparative simulation results show that the proposed CQSVD method outperforms the state of the art secret key generation methods.

- **A New Physical Layer Key Generation Dimension: Indices Based Key Generation**

In this paper, a novel algorithm for secret key generation from the wireless channel in multi-carrier systems is proposed for ensuring the confidentiality and authentication in wireless communication systems. The novelty of our proposed algorithms lies in the generation of random secret bits not just from the magnitudes of orthogonal frequency division multiplexing (OFDM) subchannels as it has conventionally been done in the literature, but also from the indices/positions of the subchannels corresponding highest gains. Thus, the proposed algorithms provides additional dimensions for enhancing overall key rates. The efficiency of the proposed algorithms is evaluated in terms of key mismatch rate (KMR) and key generation rate (KGR). Simulation results showed that the proposed algorithms can enhance the overall performance of physical layer key-based algorithms by providing extra dimension for secret key generation.

- **Enhancing Physical Layer Security of OFDM-based systems Using Channel Shortening**

  This work presents a simple, spectral and power efficient scheme for providing secure OFDM communication system using channel shortening. The basic concept is to utilize a channel shortening technique, whose design is based on the channel of the legitimate user (Bob), in such a way that the length of the effective channel is made equal to or less than the cyclic prefix (CP) at Bob only, while the length of the effective channel at the illegitimate receiver (Eve) is greater than CP. Thus, this causes inter-symbol-interference (ISI), loss of orthogonality, and overall performance degradation at Eve. The simulation results show that the presented technique can provide a significant BER performance gap between Bob and Eve, and can provide Quality of Service (QoS) based security. The design is shown to be robust against channel imperfections and can provide spectral and power efficiency beside enhancing security.

- **Adaptive OFDM-IM for Enhancing Physical Layer Security and Spectral Efficiency**

  In this paper, we propose algorithms for enhancing physical layer security and spectral efficiency of Orthogonal Frequency Division Multiplexing

(OFDM) with Index Modulation (IM) systems. Particularly, different activation ratios and/or constellation modulation orders are selected adaptively for each sub-block based on the channel quality of the legitimate receiver. More specifically, three approaches named as 1) OFDM with Adaptive Index Modulation and Fixed Constellation Modulation (OFDM-AIM-FCM), 2) OFDM with Adaptive Index Modulation and Adaptive Constellation Modulation (OFDM-AIM-ACM), and 3) OFDM with Variable Index Modulation and Variable Constellation Modulation (OFDMVIM- VCM) are proposed for enhancing physical layer security and spectral efficiency. Simulation results are presented to investigate the effectiveness of the proposed algorithms.

- **Secure and Reliable IoT Communications Using Nonorthogonal Signals' Superposition with Dual-Transmission**
  Ensuring secure communication for internet of things (IoT) has drawn much attention because of the limitation in the use of conventional cryptographic techniques owing to the unique features of IoT devices such as low complexity, lightweight computing, and power constraints. Physical layer security (PLS) has the potential to provide security solutions that are suitable for such applications. In this article, an efficient PLS approach is proposed for providing secure communication against external and internal eavesdroppers in a downlink multi-carrier IoT communication system. The system consists of a transmitter with a single active antenna (and a single radio frequency chain) that is trying to communicate with two single-antenna IoT devices in the presence of a passive eavesdropper. In the proposed algorithm, frequency selective channel based pre-coder matrices and dual-transmission approach are jointly employed to provide simple and secure communication without complex computational processing at the IoT devices. Simulation results showed that the proposed algorithm can provide security against internal and external eavesdroppers and is suitable for IoT devices.

- **Cognitive Security of Wireless Communication Systems in the Physical Layer**

While the wireless communication systems provide the means of connectivity nearly everywhere and all the time, communication security requires more attention. In the traditional wireless security, the encryption techniques are used to protect user data in the upper layers of the communication stack. Even though current efforts provide solutions to specific problems under given circumstances, these methods are neither adaptive nor flexible enough to provide security under the dynamic conditions which make the security breaches an important concern. Before the problem is moved up to the upper layers, the security demands due to ever increasing complexity of wireless communication systems and prevalence of wireless services in the daily life can be addressed by introducing new security measures in the physical layer. In this paper, a cognitive security (CS) concept for wireless communication systems in the physical layer is proposed with the aim of providing a comprehensive solution to wireless security problems. The proposed method will enable the comprehensive security to ensure a robust and reliable communication in the existence of adversaries by providing adaptive security solutions in the communication systems by exploiting the physical layer security from different perspective. The adaptiveness relies on the fact that radio adapts its propagation characteristics to satisfy secure communication based on specific conditions which are given as user density, application specific adaptation and location within CS concept. Thus, instead of providing any type of new security mechanism, it is proposed that radio can take the necessary precautions based on these conditions before the attacks occur. Various access scenarios are investigated to enable the CS while considering these conditions.

- **Secure Communication via Untrusted Switchable Decode-and-Forward Relay**

  In this paper, a practical power efficient technique is proposed for an untrusted decode-and-forward (DAF) based cooperative communication system to provide secure communication between the source and the destination. More specifically, a DAF relay, called switchable DAF (sDAF), is designed in such a way that it can be switched to amplify-and-forward (AAF)

in certain predefined situations. The algorithm is based on destination-assisted jamming and comprised of two phases. The first phase securely shares the random manipulating sequence (RMS) through an untrusted relay, while the second phase uses this RMS for secure communication through untrusted relay. This algorithm not only provides secrecy, but also enhances the power efficiency as compared to other destination-assisted jamming techniques.

- **Physical Layer Security for NOMA: Requirements, Merits, Challenges, and Recommendations**
  Non-orthogonal multiple access (NOMA) has been recognized as one of the most significant enabling technologies for future wireless systems due to its eminent spectral efficiency, ability to provide an additional degree of freedom for ultra-reliable low latency communication (URLLC) and grant free random access. Meanwhile, physical layer security (PLS) has got much attention for future wireless communication systems due to its capability to provide security without relying on traditional cryptography-based algorithms. In this article, security design requirements for NOMA and solutions provided by PLS to fulfill these requirements are discussed. The merits and challenges arising from employing PLS to NOMA are identified. Finally, future recommendations and prospective solutions are also presented.

- **Primary User Emulation and Jamming Attack Detection in Cognitive Radio via Sparse Coding**
  Cognitive radio is an intelligent and adaptive radio that improves the utilization of the spectrum by its opportunistic sharing. However, it is inherently vulnerable to primary user emulation and jamming attacks that degrade the spectrum utilization. In this paper, an algorithm for the detection of primary user emulation and jamming attacks in cognitive radio is proposed. The proposed algorithm is based on the sparse coding of the compressed received signal over a channel-dependent dictionary. More specifically, the convergence patterns in sparse coding according to such a dictionary are used to distinguish between a spectrum hole, a legitimate primary user, and

an emulator or a jammer. The process of decision-making is carried out as a machine learning-based classification operation. Extensive numerical experiments show the effectiveness of the proposed algorithm in detecting the aforementioned attacks with high success rates. This is validated in terms of the confusion matrix quality metric. Besides, the proposed algorithm is shown to be superior to energy detection-based machine learning techniques in terms of receiver operating characteristics curves and the areas under these curves.

1.4 Publications

Conference Papers:

1. 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)

2. 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)

3. 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)

4. H. M. Furqan, J. M. Hamamreh, H. Arslan, "Secure and Reliable IoT Communications Using Nonorthogonal Signals' Superposition with Dual-Transmission," IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)

5. H. M. Furqan, et. al, "Iterative Tap Pursuit for Channel Shortening Equalizer Design" Submitted to International Conference on Computer and Communication Engineering (ICCCE)

6. J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure Pre-coding and Post-coding for OFDM Systems along with Hardware Implementation," in

Proc. 13th Intern. Wireless Commun. Mob. Comput. Conf. (IWCMC)

7. M. Nazzal, H. M. Furqan, H. Arslan, "FDD Massive MIMO Downlink Channel Estimation via Selective Sparse Coding over AoA/AoD Cluster Dictionaries," IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)

8. M. A. Aygul, H. M. Furqan, M. Nazzal, H. Arslan, "Deep Learning Assisted Detection of PUEA and Jamming Attack in Cognitive Radio Systems," IEEE Vehicular Technology Conference (VTC-Fall)

9. H. M. Furqan, M. S. J. Solaija, and H. Arslan, "Intelligent Physical Layer Security Approach for V2X Communication" (Submitted to GlobeCom)

Journals:

1. H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Adaptive OFDM-IM for Enhancing Physical Layer Security and Spectral Efficiency,"Hindawi Wireless Communications and Mobile Computing

2. H. M. Furqan, J. M. Hamamreh, and H. Arslan, "A New Physical Layer Key Generation Dimension: Indices Based Key Generation", IEEE Communications Letters (under revision)

3. Haji M. Furqan, M. A. Aygul, M. Nazzal, H. Arslan, "Primary User Emulation and Jamming Attack Detection in Cognitive Radio via Sparse Coding," EURASIP Journal on Wireless Communications and Networking

4. H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical Layer Security for NOMA: Requirements, Merits, Challenges, and Recommendations, arXiV, 2020

5. J. M. Hamamreh, H. M. Furqan, et. al,, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials

6. M. H. Yilmaz, H. M. Furqan, et. al, "Cognitive Security of Wireless Communication Systems in the Physical Layer," Hindawi Wireless Communications and Mobile Computing

7. Abdulateef, Haji M. Furqan, "Smart and Secure Wireless Communications via Reflecting Intelligent Surfaces: A Short Survey", arXiv preprint arXiv:2006.14519. (IEEE OJ-COMS (under revision))

8. H. TURKMEN, M. S. J. Solaija, H. M. Furqan, and H. Arslan, "GeneralizedRadio Environment Monitoring for Next Generation Wireless Networks,"arXiv e-prints, p. arXiv:2008.06203, Aug. 2020

9. H. M. Furqan, M. S. J. Solaija, H. TURKMEN and H. Arslan, "Security for Generalized Radio Environment Monitoring for Next Generation Wireless Networks," (under preparation)

Book chapter:

- Physical layer security designs for 5G and beyond

Patents:

1. Haji M. Furqan, J. M. Hamamreh, H. Arslan, "Generic Adaptive OFDM-IM for Enhancing Physical Layer Security and Spectral Efficiency", Turkish Patent, 2018.

2. Haji M. Furqan, J. M. Hamamreh, H. Arslan, "Secure and Reliable IoT Communications Using Nonorthogonal Signals' Superposition with Dual-Transmission", Turkish Patent, 2018.

3. Haji M. Furqan, M. A. Aygül , M. Nazzal, "Jamming and Primary User Emulation Detection in Cognitive Radio Exploiting Sparse Coding Convergence Patterns", Turkish Patent, 2020.

4. Haji M. Furqan, J. M. Hamamreh, H. Arslan, "New dimension for physical layer key generation", Turkish Patent (under preparation).

Projects:

1. TÜBİTAK, "Achieving Physical Layer Security in Wireless Communication Systems", 2014-2017
2. SSB, "Cross Layer Communications Security for Cognitive Radio Networks", 2018-2020

Chapter 2

Physical Layer Security Designs for 5G and Beyond

2.1 Introduction and Motivation

Nowadays, wireless communication services are an integral part of our life due to the increasing demand for mobility and ubiquitous connectivity. These services have been employed in various beneficial civilian and military applications, where a massive amount of data generated by these applications is transmitted over the wireless media. However, communication over the wireless media is susceptible to eavesdropping, spoofing, and jamming attacks by illegitimate nodes due to its broadcast nature. Figure 2.1 presents different attacks in wireless communication by considering vehicular communication as an example. In eavesdropping, an illegitimate receiver tries to intercept the communication between legitimate parties, thus violating confidentiality and privacy. Figure 2.1 shows the example of an eavesdropper trying to access parking-related information of a user. In the case of jamming, the illegitimate node generates intentional interference to disrupt the communication between the legitimate nodes. As shown in Figure 2.1, a jammer might try to interrupt the communication between vehicles, forcing them to collide. Finally, in the spoofing attack, the control of the communication

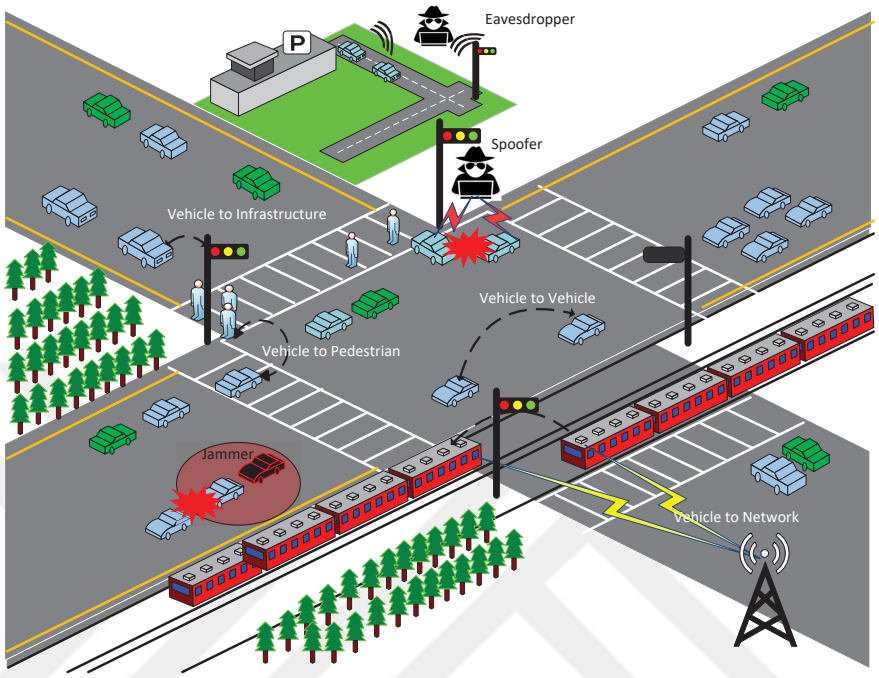


Fig. 2.1: An overview of different security threats in wireless communication. Jamming is shown to disrupt communication, while spoofing can manipulate the interaction between entities to cause accidents. An eavesdropper is shown to capture vehicle information at parking.

channel between the legitimate parties is taken by a spoofer, which can replace, modify, and intercept the messages that are being transmitted between legitimate parties. A spoofing attack on vehicular communication might result in vehicles moving in direct collision paths of each other, as shown in Figure 2.1.

In all developed wireless communication systems and standards such as second-generation (2G), third-generation (3G), fourth-generation (4G), fifth-generation (5G), wireless fidelity (WiFi), worldwide interoperability for microwave access (WiMax), wireless gigabit (WiGig), etc., the main objectives of the physical layer (PHY) transmission techniques and schemes have mainly been focused on achieving two key design requirements: 1) increasing data rates (higher capacity and spectral efficiency), and 2) enhancing reliability (lower error rates) along with reducing latency. These two key design requirements have been the primary driving factors for research and development in wireless communications in recent times. In fact, these requirements related to spectral efficiency and reliability are usually

fulfilled by using novel PHY-transmission techniques; while leaving security as an out of scope requirement that is left to be handled by upper layers. This conventional design paradigm has resulted in two phenomena: 1) what is called add-on security (i.e., security is an additional overhead added to different open systems interconnection (OSI) layers), and 2) making security requirement a computer engineering issue rather than being a joint computer-telecommunication issue as it must be. Consequently, the security services such as confidentiality and authentication have conventionally been achieved so far at the upper layers such as application (APP), transport (TRN), network (NET), and media access control (MAC) layers [7].

For instance, to ensure the authenticity of a receiver, existing wireless systems typically employ multiple authentication approaches simultaneously at different layers, including MAC layer authentication, NET layer authentication, TRN layer authentication, and APP layer authentication. A similar example applies to confidentiality, i.e., data protection from eavesdropping, where multiple confidentiality approaches are usually employed at different layers simultaneously to prevent data leakage to eavesdroppers. Particularly, at the application-presentation layer, we have secure shell (SSH), where encryption is in support of secure file transfer protocol (SFTP), secure hypertext transfer protocol (SHTTP), pretty good privacy (PGP), and secure/multipurpose internet mail extensions (S/MIME). At the transport layer, we have a secure socket layer and transport layer security (TLS). At the network layer, we have internet protocol security (IPSec), encapsulating security payload (ESP), and IPSec tunnel ESP, which can be supported by standard encryption algorithms such as data encryption standard (DES) and advance encryption standard (AES). At the MAC layer, we have WiFi protected access (WPA) and temporal key integrity protocol (TKIP). Obviously, this multilayer security approach is costly and inefficient as it creates significant network bottlenecks, latency, signaling overhead, and increases computation complexity, especially for future wireless systems that are expected to provide highly secure, delay-sensitive, and low complexity applications and services such as internet of things (IoT)-based services including massive machine-type communications (mMTC) and ultra-reliable low latency communication (URLLC) [7].

To address these challenges, physical layer security (PLS) [12] is proposed as a complementary solution to cryptography-based solutions that aims to provide security as an inherent and built-in feature of the PHY-transmission mechanism. This approach results in the need to design novel transmission techniques that consider achieving the Quality-of-Service (QoS) requirements for different services/applications at the lower PHY in terms of not only reliability, capacity, and latency, but also security. Therefore, security, in this case, will be applied to the physical signals carrying the data bits, rather than being applied to the data bits themselves, which are carried by the transmit electromagnetic waves as is the case in upper layers cryptography approaches.

To deliver security at the PHY, PLS approaches exploit the dynamic characteristics of the wireless channel such as channel randomness, interference, noise, fading, dispersion, diversity, separability, reciprocity, etc., along with radio frequency (RF) front-end-associated impairments to prevent the illegitimate node from decoding data while ensuring that the legitimate user can decode it successfully [12]. Moreover, PLS is employed to confirm the authenticity of communication entities at the PHY in order to protect against spoofing attacks [7] and is also employed to enable reliable communication during jamming attacks.

PLS security introduces an additional degree of freedom in terms of dynamically adjusting the complexity, latency, and efficiency of communication systems. This can be achieved by providing various flexible options regarding the functionality split between PHY and upper layers using an intelligent security engine. More specifically, such an engine can be used to adjust and maintain the security functionalities of different layers jointly to enhance overall security while ensuring the other requirements of communication systems such as complexity, delay, latency, and efficiency.

In addition to the aforementioned key motivation behind PLS, we also have the following reasons that motivate the continuous research efforts on PLS compared to cryptography. These reasons are summarized below:

- The key distribution and management processes for the legitimate parties

in conventional encryption-based systems are cumbersome and unfeasible in large-scale, dense, and heterogeneous wireless networks as is the case in the future beyond 5G systems, where a massive number of smart devices are simultaneously connected to the network. This causes excessive complexity, high signaling overhead, and costly computational processes. Also, the management and exchange of control frames between communication entities are usually not very well protected.

- Longer key length, which is usually preferable in cryptography approaches to increase the security strength, results in more waste of resources, apart from the fact that implementing security methods with Shannon's perfect secrecy is hard to be practically achieved with today's huge data volume. For instance, to perfectly secure a message of 10 gigabytes in practice, we need to share and use a key of the same size and use it only once. When we transmit another message, we must generate another key and so on, which is costly and inefficient.

- The fast developments and advances in computing power devices reveal the fact that the current secret key-based techniques can be cracked, no matter how mathematically complex they are, especially when quantum computing becomes a reality [12]. This would make all currently used encryption-based algorithms at risk and consequently all the applications that depend on using these algorithms for security.

- Cryptography-based security causes extra delay, consumes excessive computational power, and increases complexity, making it inefficient and unsuitable to the IoT-based Tactile communication applications such as autonomous driving, remote surgery operation, controlling the unmanned aerial vehicle (UAV), etc. These future applications require the utmost security with minimal latency. Particularly, given the extremely wide range of IoT-based wireless applications including industrial, medical, commercial, governmental, and military applications, designing practical security techniques is becoming an indispensable need for future wireless systems.

- Besides, future mobile base stations (BSs), as well as mobile devices and

handsets (especially IoT devices), are expected to be noticeably different from the existing ones in terms of requirements, hardware capabilities, and channel nature. Thus, their security requirements and designs are also going to be significantly different.

All of these issues together motivate the development and design of new practical complementary security techniques at the PHY to protect and safeguard future wireless transmissions. Hence, the main goal of this chapter is to provide a coherent overview and deep insights on PLS concepts against eavesdropping, spoofing, and jamming for future wireless networks. In the first part of the chapter, anti-eavesdropping techniques are presented. We classify the existing PLS techniques against eavesdropping into two primary classes: signal-to-interference-plus-noise ratio (SINR)-based class, which includes key-less PLS approaches, and complexity-based class, that includes key-based PLS approaches.

The techniques belonging to each of these classes are discussed and explained in time, frequency, and space domains with examples and illustrations. The merits and demerits of each approach alongside important lessons are also discussed. Moreover, secrecy notions and secrecy performance metrics are also elaborated. Furthermore, the recent applications of PLS to different emerging wireless technologies such as millimeter-wave (mmWave), massive multiple-input multiple-output (mMIMO), URLLC, IoT, UAV, and cognitive radio (CR) are also presented. In the second part of the chapter, we cover and discuss the details about PLS beyond content secrecy including PHY-authentication methods against spoofing attacks and details about jamming attacks and related solutions. The chapter is concluded with future research directions and recommendations.

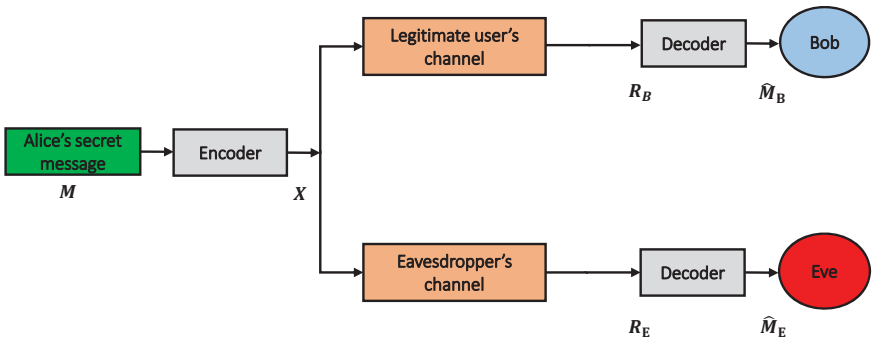


Fig. 2.2: Generic system model of PLS related to eavesdropping problem in which Alice tries to communicate confidentially with Bob without allowing Eve to get any useful information from the ongoing communication.

2.2 Fundamentals, Preliminaries, and Basic System Model for PLS

The basic foundation of the secrecy system was laid by Shannon in [13] which has since been extensively used for providing secure communication. However, it is based on cryptography-based approaches that face many challenges concerning future communication systems as explained in the aforementioned discussion. In order to solve all or some of the issues faced by the cryptography-based security system, key-less based security approaches had emerged as effective solutions. The first work in this direction is presented in [14] by Wyner and is considered as a foundation of the research on key-less PLS. The basic idea in Wyner's approach was that the secure communication between two legitimate parties can be achieved if the illegitimate receiver's channel is a degraded version of the legitimate receiver's channel. The security, in this case, is achieved by employing channel-dependent stochastic encoders. Inspired by Wyner's work, many research studies and works have been proposed in the literature for different communication scenarios and channel types [12].

Figure 2.2 presents a generic model for PLS, which consists of a legitimate

transmitter (Tx), Alice, that is trying to communicate securely with the legitimate receiver (Rx), Bob, in the presence of an illegitimate receiver (eavesdropper), Eve, who wants to decode and interpret the message that is intended for the legitimate receiver. Moreover, due to the spatial de-correlation property of wireless channels, legitimate and illegitimate nodes are assumed to experience independent channels if they are at least half a wavelength apart.

To explain PLS more clearly, let's assume that Alice wants to send a message through the wireless channel. In the first step, Alice encodes the message M and then sends a resultant encoded message X through the wireless channel. The received signal at the legitimate receiver is represented by R_B while at the illegitimate receiver it is represented by R_E. Finally, Bob and Eve decode their received signals to get $\hat{M}_B$ and $\hat{M}_E$, respectively, as estimated versions of the transmitted message, M. The goal of PLS is to design different methods by exploiting the dynamic features of wireless communications, such as channel randomness, dispersion, interference, fading, noise, etc. along with the architecture of transceiver including hardware impairments, estimation, etc. to prevent the eavesdropper from decoding data while ensuring that the legitimate user can decode it successfully.

The availability of the channel state information (CSI) at the transmitting nodes can be exploited to enhance the security and performance of wireless communication. In PLS literature, it is assumed that the legitimate transmitter can have (full/partial) knowledge of the CSI corresponding to the legitimate receiver. The legitimate transmitter can attain the CSI by exploiting feedback in case of the frequency division duplex (FDD) system or by exploiting channel reciprocity property in case of time division duplex (TDD) system [12].

In general, there are two types of eavesdroppers: 1) internal, and 2) external [15]. Internal eavesdropper is from the set of legitimate users of the network, while the external one is not from that set. The eavesdropper can be considered as 1) active, or 2) passive. The active eavesdropper can interrupt wireless communication by launching jamming or channel estimation attacks while passive eavesdropper just spies on the communication without interfering with the

ongoing communication [16].

2.3 Secrecy Notions and Performance Metrics

In this section, the details about the secrecy notions and performance metrics for PLS are presented.

2.3.1 Secrecy Notions

In PLS, different security algorithms provide different levels of security that can be described by secrecy notions as design criteria. The popular notions of security include perfect secrecy, weak secrecy, and strong secrecy [12]. Based on Shannon's work, the communication is said to be perfectly secure if the capacity of the legitimate receiver is equal to the secrecy capacity (zero information leakage to illegitimate node) for any code length. However, when the code length is sufficiently long enough, this will result in what is called as strong secrecy. On the other hand, Wyner's work assumed that the communication is perfectly secure if the secrecy capacity has a positive value with a certain probability, irrespective of the value of capacity of the illegitimate node. Thus, this notion of secrecy is known as weak secrecy. In addition to perfect, strong, and weak secrecy; there are also other notions for secrecy such as semantic secrecy and ideal secrecy. The conceptual and mathematical meaning of most commonly used secrecy notions are as follows:

2.3.1.1 Perfect Secrecy

It is the most stringent measure for secrecy which ensures that the amount of mutual information leakage to the eavesdropper is zero irrespective of its computation capabilities and processing power. It can be given as follows:

$$I(M; R_E) = 0, \tag{2.1}$$

$$H(M) = H(M|R_E), \tag{2.2}$$

where $I(M; R_E)$ is the mutual information between M and R_E, $H(M)$ presents the entropy of the information, while conditional entropy for the eavesdropper's observation is denoted by $H(M|R_E)$.

2.3.1.2 Strong Secrecy

The communication is said to be strongly secure if the increase in the length (n) of the codeword to infinite causes the asymptotic mutual information to approach zero values. More specifically, it forces $I(M; R_E)$ to be zero on each channel use and can be given as follows:

$$\lim_{n\to\infty} I(M; R_E) = 0. \tag{2.3}$$

2.3.1.3 Weak Secrecy

The communication is said to be weakly secure if the increase in the length (n) of the codeword to infinite causes the asymptotic mutual information rate to approach zero values. More specifically, it does not require $I(M; R_E)$ to be zero on each channel use but only on average and can be given as follows:

$$\lim_{n\to\infty} \frac{1}{n} I(M; R_E) = 0. \tag{2.4}$$

2.3.1.4 Semantic Secrecy

It means that the random guess of any function of the message, without considering the distribution of message or observation of the eavesdropper, is the best estimate asymptotically. Moreover, it is impossible to estimate better than that. It can be given as follows:

$$\lim_{n\to\infty} max_{pm} I(M; R_E) = 0, \tag{2.5}$$

where pm represents all possible message distributions.

2.3.1.5 Ideal Secrecy

The communication is said to be ideally secure if the increase in the length (n) of the codeword to infinite does not cause the asymptotic conditional entropy of the message and the key to approach zero values. More specifically, in this case, there is no unique solution of the plain text irrespective of the amount of ciphertext intercepted by Eve. It can be given as:

$$\lim_{n\to\infty} H(M|R_E) \neq 0, \tag{2.6}$$

$$\lim_{n\to\infty} H(K|R_E) \neq 0, \tag{2.7}$$

where K is the secret key sequence.

2.3.2 Secrecy Performance Metrics

In PLS, proper quantization and evaluation of secrecy performance for any designed security algorithm are among the most important steps, which can be done efficiently by using appropriate security metrics. There are two major classes of security metrics for PLS: 1) SINR-based, and 2) complexity-based. The SINR

based class is for the key-less PLS algorithms, while the complexity-based class is for key-based PLS algorithms.

The SINR based class includes packet error rate (PER) and bit error rate (BER) based metrics, secrecy throughput, secrecy capacity, and secrecy outage probability (SOP).[1] One of the most popularly used metrics is secrecy capacity, which is the difference between the channel capacities of the legitimate node and illegitimate node [17]. It should be noted that the secrecy capacity metric presents the achievable bounds of secrecy by assuming the wireless channel's random behavior. However, the actual secrecy performance can be obtained by using the difference between the error probability rates of a legitimate and illegitimate node such as PER and BER. Moreover, secure throughput and secrecy channel capacity can be directly linked with PER and BER. In order to measure secrecy in a fading environment, the researchers extended the secrecy capacity metrics to outage secrecy rate or SOP for the cases when Eve's channel is unknown. The SOP is the probability that the value of the secrecy rate is less than the minimum required threshold value of secrecy rate [17].

On the other hand, in the case of key-based PLS algorithms, the illegitimate receiver can employ a brute force attack using the exhaustive search method. Hence, the complexity-based metric is a good fit for these types of techniques. In key-based PLS methods, it is desirable to have longer keys with uniform distribution and high entropy. Moreover, to measure the effectiveness of the key-based method on the performance of the system, the key mismatch probability between the communication parties is used [18]. It should be noted that the probability of error at the illegitimate user is not a good metric for key-based methods as it cannot fulfill the requirements of secrecy in these methods.

[1]The mathematical details about the popular metrics for PLS are explained in Chapter 19.

2.4 Popular Security Techniques

In this section, we present detail about the classification, concepts, merits, and demerits of PLS techniques against eavesdropping. PLS approaches can be broadly classified into SINR (key-less)-based and complexity (key)-based approaches. SINR-based techniques include secure channel coding design, channel-based adaptation and optimization, and artificial interfering/noise-based approaches. On the other hand, the complexity-based approaches are divided into two main classes based on the layer at which the extracted secret sequences are applied.

2.4.1 PLS based on Secure Channel Coding Design

2.4.1.1 Concepts, Merits, and Demerits

The foundation of channel coding based secure communication was proposed by Wyner [14] and is the first work in the direction of key-less based secure communication. The basic idea is that the secure communication between the legitimate entities can be achieved by employing channel-dependent stochastic encoders if the illegitimate receiver's channel is a degraded version of the legitimate receiver's channel. The basic advantage of this approach is that it can solve many problems related to conventional cryptography-based as explained in section 2.1. However, Wyner based work also has some drawbacks. Firstly, it was assumed that illegitimate users will always have a degraded version of the channel compared to the legitimate user. However, in practice, illegitimate user's channel conditions can be better than the legitimate user's channel due to the random nature of the wireless channel. Secondly, there will be some loss in the throughput and capacity to achieve secrecy in this approach.

To this end, popular secure channel coding designs include low-density parity-check (LDPC) codes and polar codes [16]. The use of these codes for security augmentation is depicted in [19], where the authors make use of nested sparse graph-based LDPC codes. These codes help in achieving the secrecy capacity

when Bob's channel is noiseless whereas Eve's channel is a binary erasure channel (BEC). We find another interesting example of this approach in [20], where the authors make use of polar codes that achieve the secrecy capacity for a wide range of wiretap channels. However, the presented scheme is valid only when both the main and the wire-tap channels are binary symmetric channels.[2]

2.4.1.2 Learned Lessons

Most of the security codes studied in the literature [16] are based on the assumption of having infinite block length. However, this assumption is less practical for the case of URLLC and multimedia-based communication because of finite block length and latency constraints in them. Therefore, there is a need for the design of realistic codes for practical situations, where a finite block length is considered [21], and the secrecy rate does not need to be exactly equal to the main channel capacity. However, the design of these practical codes will face some challenges, especially if it is required to comply with the practical constraints including delay, throughput, and complexity. Additionally, to the best of our knowledge, the design of secrecy codes without taking into account the information on the eavesdropper's channel is unclear and not addressed by the literature. Therefore, the need of the hour is to come up with a novel coding technique to address the problems mentioned earlier.

2.4.2 Channel-Based Adaptation and Optimization for PLS

2.4.2.1 Concepts, Merits, and Demerits

Concept: The basic idea of this approach is to adapt and/or optimize the transmission-based on the requirements, location, and fading channel conditions

[2]For having more detailed information about channel coding based PLS, we refer the reader to [16].

of the legitimate receiver. Therefore, Bob's SINR is better than that of Eve's SINR as the transmitted signal is optimized for Bob's channel and not for Eve's channel, who happens to experience a different channel. Moreover, there is no need for any extra processing at Bob's end to decode the data in this approach. However, this approach requires full or partial knowledge of CSI of the legitimate receiver at the transmitter. Figure 2.3 presents a basic representation of the channel-based adaptation and optimization approach for PLS.

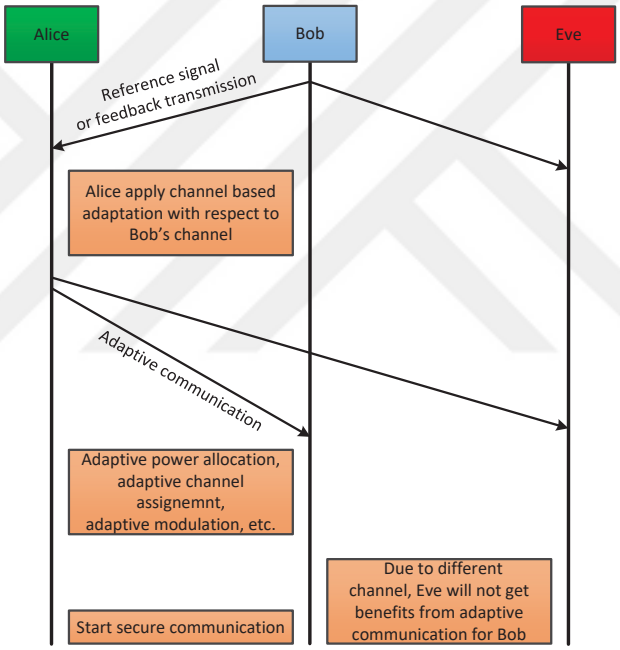


Fig. 2.3: Channel-based adaptive transmission for PLS, where basic idea is to adapt and optimize the transmission based on the requirements, location and wireless fading channel conditions of the legitimate receiver.

In addition to the feedback knowledge of the CSI at Alice, other useful feedback mechanisms can be beneficial for enhancing security. These include but are not limited to acknowledgment (ACK) and negative acknowledgment (NACK) messages in the automatic repeat request (ARQ) process, received signal strength indicator (RSSI), pre-coding matrix indicator (PMI), a rank indicator (RI) in multi-antenna systems, etc. Signaling information by partial/full CSI or feedback allows the transmitter to meet the legitimate receiver's requirements as well as makes the signal appear to be un-optimized with respect to the eavesdropper.

For example, in order for the signal to be optimized for the legitimate receiver, the transmitter can utilize adaptive waveforms and pulse shaping, adaptive resource allocation, adaptive scheduling, adaptive interleaving, adaptive modulation and coding, adaptive power allocation, and pre-coding, etc. based on signaling information.

Merits: Apart from enhancing PLS, this approach also improves efficiency, saves power, and augment Bob's reliability. Additionally, the technique can be used in FDD, TDD, or hybrid division duplex systems. Moreover, security will always be maintained at a specific level such that, even if Eve knows the feedback, it cannot benefit much from it. Furthermore, it does not require extra processing at the receiver which makes it suitable for IoT systems.

Demerits: Despite the approach being free and not requiring extra processing power (a desirable feature in future technologies and IoT devices), it requires full or partial CSI at the transmitter. These techniques may not be of much use in the case of multiple collaborative eavesdroppers that can capture different copies of the signal. A promising course of action can be the amalgamation of these techniques with other efficient security techniques with hopes of developing and maintaining an adequate secrecy level against multiple collaborative eavesdroppers.

2.4.2.2 Examples in Time, Frequency, and Space Domains

The techniques based on channel adaptation can be categorized into time, frequency, and space domains.

In the time domain, the information-carrying signal is transmitted and received by making use of a single antenna and one carrier frequency [1, 22]. In [1], for example, a secure waveform called orthogonal transform division multiplexing (OTDM) waveform is proposed. Here, the authors particularity make use of orthogonal transform basis functions extracted from the legitimate channel to modulate and demodulate the data symbols securely. A brief description of the

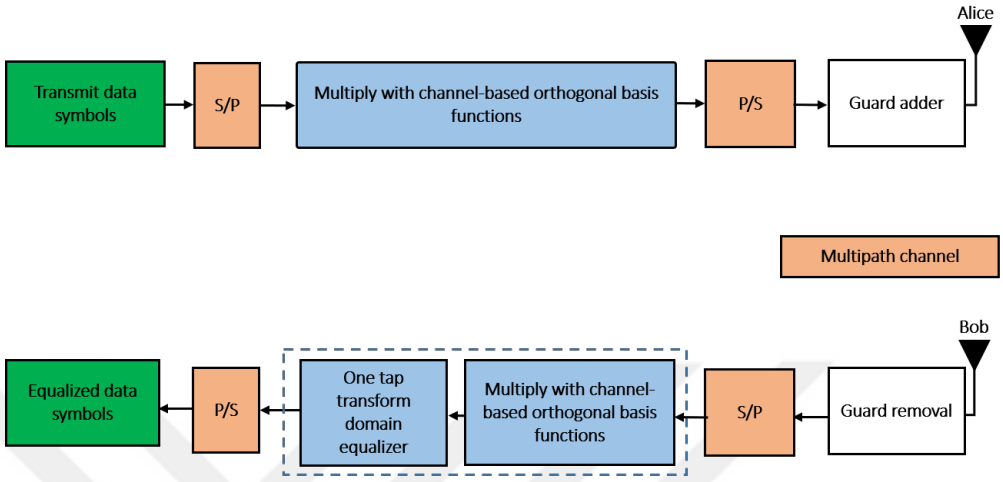


Fig. 2.4: The transceiver structure of secure OTDM waveform proposed in [1], where orthogonal transform basis functions extracted from the legitimate channel are used to modulate and demodulate the data symbols securely.

OTDM waveform is presented in Figure 2.4. The proposed design in [1] assures a reliability gain in addition to security over OFDM.

Frequency domain can also be utilized for channel adaptation based techniques. In this domain, by making use of a single antenna, a one-time slot or a block of data symbols is transmitted and received over several subcarrier [23, 24]. For example, in [24], the authors propose a technique called OFDM with subcarrier index selection (OFDM-SIS) and adaptive interleaving. In the scheme, the entire OFDM block is divided into smaller sub-blocks each experiencing good and bad sub-channels. To enhance the signal-to-noise ratio (SNR) at the legitimate receiver only, this scheme makes use of an optimal channel-based selection of the subcarrier indices in each sub-block. It can be seen that the OFDM-SIS scheme not only improves and enhances the secrecy performance but also enhances reliability for the legitimate user. In doing so, the scheme saves power and reduces complexity, which makes it an appropriate contender for 5G URLLC service.

In the space domain, the signal of interest consists of a one-time slot, one carrier frequency, but several spatial transceiver sources (i.e., antennas). In general, the space domain includes MIMO, multiple-input single-output (MISO), single-input multiple-output (SIMO), distributed antenna system (DAS), coordinated

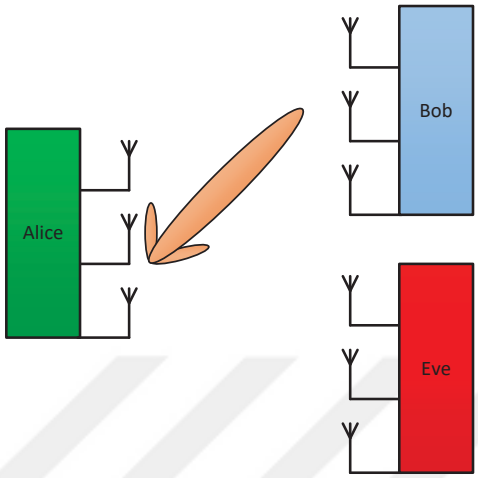


Fig. 2.5: The basic beamforming approach that is based on the idea of the signal's power enhancement at the legitimate user and its suppression in the other directions.

multipoint (CoMP) systems, relays, reconfigurable intelligent surface (RIS), and so on. Secrecy can be provided via adaptation techniques in the space domain too based on the above-mentioned concepts. Several techniques can be used to realize and exemplify the security in space domain such as adaptive power allocation, transmit antenna selection, beamforming, interference alignment, pre-coding (zero forcing, geometric mean decomposition, minimum mean squared error, and generalized singular value decomposition), full/partial pre-equalization, relay selection, RIS phase optimization, and so on. In [25], for example, beamforming based security approach is presented that is based on enhancing the signal power at the legitimate user and suppressing it in other directions, as illustrated in Figure 2.5. In [26], the authors discuss the directional modulation based multi-antenna security concept. The basic idea of this scheme involves the relative positions of the constellation points. More specifically, the constellation points maintain their positions relative to each other in the desired direction; however, they get jumbled in phase and amplitude at undesired directions. Therefore, the performance at Eve undergoes degradation despite getting the same signal power. The basic concept of directional modulation for PLS is presented in Figure 2.6. Moreover, when the space domain is concerned, the relays offer good contenders for channel adaptation based security techniques. Relays create an

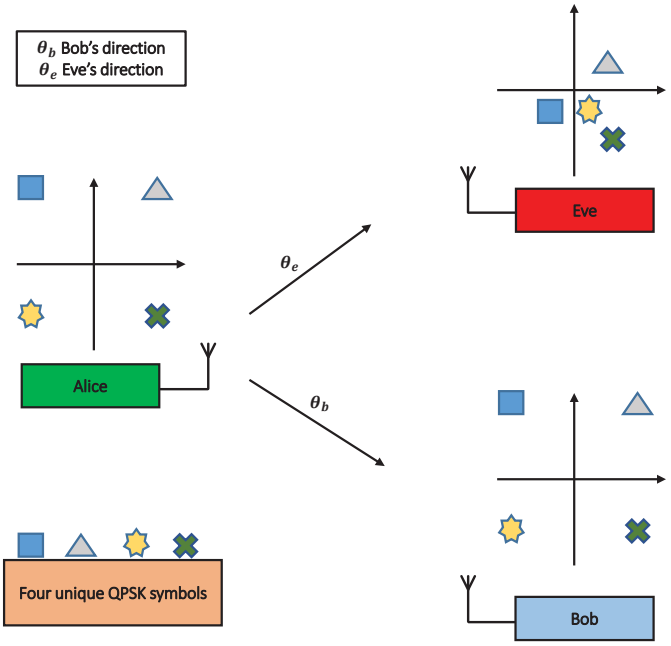


Fig. 2.6: PLS using directional modulation, where the constellation points maintain their positions relative to each other in the desired direction only.

additional path to the source through which the signal is transmitted to the destination [27]. This additional degree of freedom can be exploited for enhancing the overall security of the system. For example, in [28], a beamforming system based on collaborative use of relays is designed to maximize the secrecy capacity. In this scheme, some nodes are used for jamming to degrade the performance of legitimate users while other nodes are used for beamforming.

2.4.2.3 Learned Lessons

The majority of the adaptation based security schemes emphasize upon the optimization of the PHY-transmission parameters in accordance with the channel characteristics. However, there is not much thought given to the upper layer parameters based on secrecy requirements in this process. Specifically, the notion of cross-layer security design comprising the interaction between different layers from a PHY-perspective is not yet well studied in the literature: 1) Cross

MAC-PHY-security: This approach involves the maximization of secrecy alongside meeting the QoS requirements of the legitimate users. This is achieved by the joint optimization of the MAC functionalities including resource allocation, scheduling, hybrid ARQ, multiplexing, prioritization, etc. The work in [2] highlights a study that incorporates an example of this area of research. The study highlights the joint design of AN and ARQ functionality to enhance security. 2) Cross NET-PHY-security: This concept makes use of the collective optimization of network layer functionalities including switching from one node to another, relaying, and routing along with the PHY-parameters to enhance the secrecy. A study built upon this concept is highlighted in [29]. The paper discusses the design of a power-efficient and secure routing protocol. 3) Cross APP-PHY-security: This concept is based on the adjustment of PHY-transmission parameters in accordance with the channel and the running applications at the user side. The data rates and sensitivity to the error of these applications are also taken into account in a way to enhance the secrecy of the overall system. An example of APP-PHY-security is presented in [2].

2.4.3 Addition of Artificial Interfering (Noise/Jamming) Signals for PLS

2.4.3.1 Concepts, Merits, and Demerits

Concept: The basic idea in this approach is that an interfering signal (called artificial noise (AN) or jamming) is added by a trusted node such as Alice, Bob, or a third party to degrade Eve's performance. This approach makes use of the channel's null space of the legitimate user to add interference signals. In case when there is no null space in the channel, the transceiver structure can be exploited (such as combiners, filters, pre-coders, equalizers, etc.) along with the help of diversity to add artificial interference signal.

Merits: One of the biggest advantages of this approach is that very strong

security can be realized at any distance from the source in both fading and non-fading environments by employing it. The additional benefit for this approach can be seen in the fact that neither does it require extra processing at the receiving end nor does it increase complexity, making it backward compatible with the current handheld devices. Furthermore, this approach can be applied to FDD and TDD systems. And of course, in addition to secrecy, the added interfering signals can provide added benefits which include a reduction in peak-to-average power ratio (PAPR) and the mitigation of the adjacent channel interference and out-of-band emission (OOBE).

Demerits: Like any other scheme, this too comes with its tradeoff. Injection of an interfering signal requires the CSI knowledge at the transmitter and it also causes little degradation in the channel capacity alongside the sacrifice of the power resources. This degradation in the channel capacity is also observed due to the loss of a degree of freedom in order to provide security. A little degradation in the performance might also occur at the legitimate receiver due to channel estimation errors. Moreover, if the AN signal is not properly designed, it may also cause an increase in PAPR.

2.4.3.2 Examples in Time, Frequency, and Space Domains

The addition of artificial interfering based techniques can be further divided into time, frequency, and space domains.

Considering the artificial interfering techniques in the time domain, the procedure involves the addition of the interfering signal on top of the information signal in such a way that the signal gets canceled out only at the desired receiver while causing a severe degradation at the eavesdroppers. An interesting work related to AN is proposed in [30], where the operation is performed in the time domain. As seen in Figure 2.7, this technique uses OFDM as a transmission scheme, and the transmitted signal is added with a properly designed AN in such a way that AN gets accumulated over the cyclic prefix (CP) part of the signal at the only legitimate receiver when it passes through frequency selective channel. Therefore,

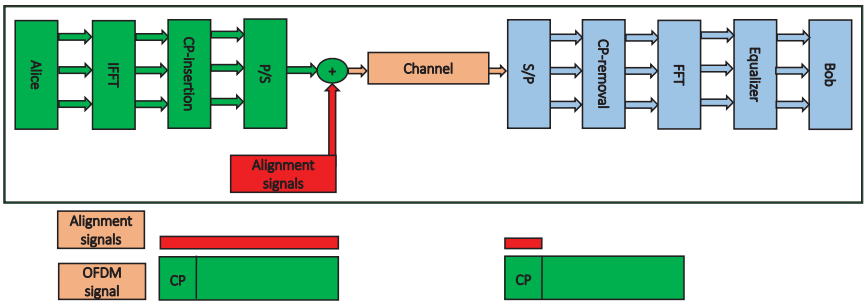


Fig. 2.7: An OFDM transceiver structure with AN addition in the time domain, where the transmitted signal is added with a properly designed AN in such a way that it gets accumulated over the CP part of the signal at the only legitimate receiver when it passes through frequency selective channel.

this allows Bob to get rid of the noise automatically when the signal is processed to remove the CP part of the OFDM signal. Contrary to this, signal degradation is observed at Eve's end because AN is designed based on the degree of freedom provided by CP with respect to Bob's channel.

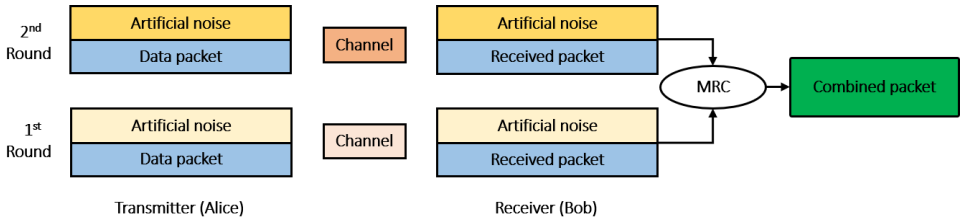


Fig. 2.8: Design structure of ARQ with AN scheme proposed in [2] for providing secure communication.

It should be noted that the implementation of the time domain AN schemes in [7] are applicable to the SISO systems in case of rich scattering channels. In addition to this, the secrecy performance of these techniques improves with the increase in the number of channel taps. However, if the channel happens to have a single tap, none of the above-mentioned schemes is successful in providing secrecy. To negate this dependency, an efficient algorithm is proposed in [2] that successfully provides secrecy even in the presence of a single tap. This is achieved by adding a specially designed AN on top of each transmitted data packet by exploiting ARQ protocol along with maximum ratio combining (MRC). More specifically, the re-transmission process in ARQ is designed in such a way that, when the same packet is requested by Bob, a specially designed AN canceling

signal is added to the next re-transmission round. This results in the reception of an AN-free packet at the legitimate receiver by means of the MRC process. On the other hand, the performance at Eve is significantly reduced due to AN. Figure 2.8 represents a brief structure of ARQ with AN scheme.

As far as the frequency domain is concerned, the addition of the designed interfering signal can also be done without degrading the performance of the desired receiver. An example of this is quoted in [31], where the author exploited faded subcarriers of OFDM systems to add AN instead of data to confuse the eavesdropper. As the eavesdropper has a different channel than that of Bob, thus it cannot distinguish between subcarriers filled with AN from those used to carry the data symbols. This ultimately results in the degradation in the channel capacity and performance of eavesdropper based on the number of sub-channels filled with AN.

There are a lot of interesting works in the literature in the space domain based on the concept of AN [32]. The security techniques in the literature cover the majority of scenarios of space domain such as SIMO, MISO, MIMO, DAS, CoMP, relays, RIS, etc. An example is presented by Goel and Negi in [32], where multiple antennas are used to implement AN based algorithm, as depicted in Figure 2.9. In order for this technique to be successful, two conditions must be fulfilled: 1) there should be a null space in the channel and for that, the number of transmit antennas must be greater than that of legitimate receiver antennas, and 2) in order to ensure that Eve cannot align the added noise, the number of antennas at Eve must be less than that of Alice. Relay assisted interference techniques are also popular security techniques. For example, interference/jamming signals can be sent to the eavesdroppers via relays to prevent them from receiving the secret message [33], as illustrated in Figure 2.10. Moreover, in cases when the relay is untrusted yet enhances the reliability of the scheme [34], the destination can be used to jam the relay in a way such that the reliability is improved but the information from the signal can not be extracted by the relay, as presented in the Figure 2.11.

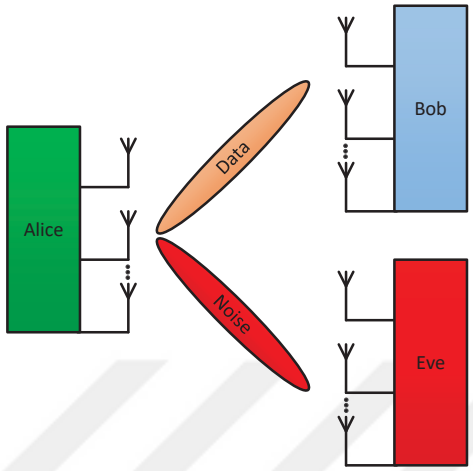


Fig. 2.9: A MIMO wireless system with Alice, Bob, and Eve, each having multiple antennas. Alice exploits multiple antennas to add AN in the null space of the channel.

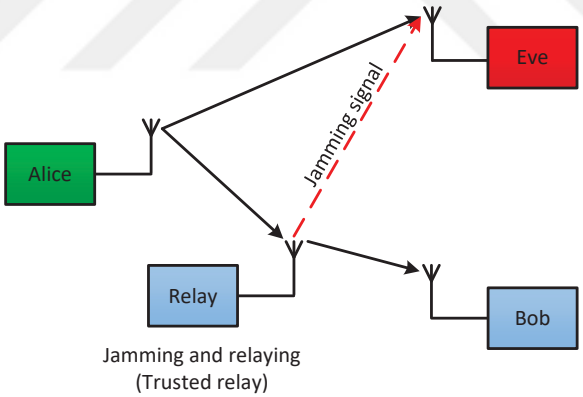


Fig. 2.10: Cooperative jamming of eavesdropper with AN by trusted relay.

2.4.3.3 Learned Lessons

While the above-mentioned studies that deal with AN concentrate mainly on enhancing the secrecy capacity, a little attention is paid to the underlying constraints that might hinder the practical realization of these techniques. For instance, an increase in the PAPR due to additive white Gaussian noise results in several issues. These issues include, but are not limited to out-of-band and in-band interference, power inefficiencies, inter-modulation product generation, and coverage range reduction. Therefore, it is crucial to consider and understand the

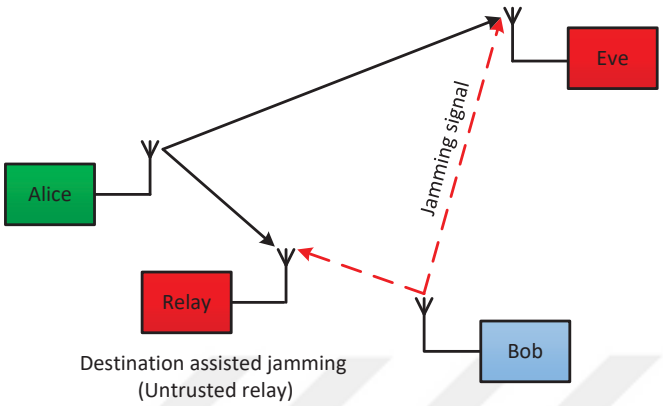


Fig. 2.11: Cooperative jamming of eavesdropper and untrusted relay with AN.

practical constraints to properly design interference signal such that the proposed strategies are also applicable in real-world situations.

2.4.4 Extraction of Secret Sequences from Wireless Channels

2.4.4.1 Concepts, Merits, and Demerits

Concept: The proposed security approach comes into action when both the transmitter and receiver generate secret keys (random sequence vectors or matrices) from legitimate channel link [35]. The legitimate parties can exploit the phase and amplitude of channel impulse response (CIR), RSSI, and other feedbacks for key generation.[3] The fundamental assumptions at the back end of the key-based approach are as follows: 1) channel decorrelation, which implies that the legitimate and the illegitimate nodes who are positioned at least half-wavelength apart will experience channel responses that are independent of each other in a rich scattering environment, 2) channel reciprocity, where same channels at the ends of a link can be used to generate similar keys at both ends, 3) channel randomness in temporal, spectral, and spatial domains, due to multipath

[3]Note that the techniques mentioned in this section are applicable for both confidentiality and authentication purposes. The detail about authentication is presented in section 2.5 of this chapter.

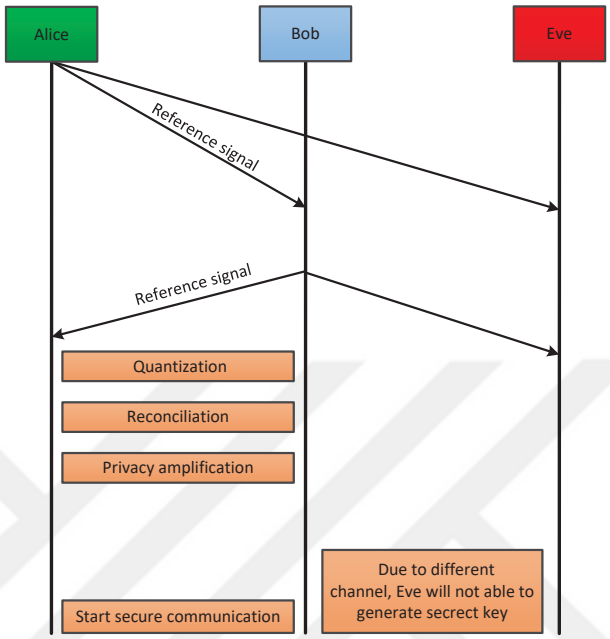


Fig. 2.12: Basic steps for secret key generation from the legitimate wireless channel including channel estimation, quantization, reconciliation, and privacy amplification.

propagation in a rich-scattering environment.

Figure 2.12 presents the primary steps for secret key generation. The details of these steps are given as follows: 1) probing the channel at both ends of the link to generate random correlated measurements using sounding techniques, 2) mining channel features and using them as shared random variables, 3) generating secret random keys via channel quantization, 4) applying reconciliation to minimize mismatch in the key, and 5) conducting privacy amplification to optimize the overall randomness of the key.

Merits: The key aspects that have motivated and influenced the research on the channel-based key are as follows: 1) overcoming the key management issues such as those involving distributing, sharing, and storing of keys, 2) this approach works even when Eve might have good channel conditions compared to Bob.

Demerits: This particular method cannot be extended to practical situations for achieving a flawless Shannon's notion of secrecy since the number of random

bits generated is constrained by variations in the channel. Nonetheless, they can be broken down by quantum computing. Moreover, it is worth stating that this approach is prone to channel reciprocity mismatch and imperfect channel estimation which negatively impacts overall performance. This channel reciprocity mismatch stems from the difference in hardware impairments at Alice and Bob. It can also result due to different interference levels in the uplink and downlink. Hence, it becomes necessary to integrate robust channel calibration techniques along with reconciliation approaches to overcome these problems. It should be noted that this approach requires additional signaling and add-on processing at both Alice and Bob, giving rise to the need for a complex processing infrastructure that increases overheads and causes further delays. It is also worth mentioning here that this approach is limited to TDD systems and there is very little work related to FDD based key generation. Finally, this approach is ineffective in cases where there is a lack of variations and randomness in the channel such as in the line-of-sight (LOS) or poor scattering environments.

2.4.4.2 Examples in Time, Frequency, and Space

The techniques based on key generation can be categorized into time, frequency, and space domains.

Time domain deals with the generation and extraction of random keys by Alice and Bob with respect to variations of the channel as a result of fading, interference, dispersion, and noise in time domain [36, 37]. For instance, in [36], secret bits have been extracted from RSSI and CIR measurements through quantization. Another example in this scenario pertains to the manipulation of single-bit feedback messages (ACK and NACK) from the ARQ protocol for key generation [37].

Frequency domain can also be used for efficient secret key generation in a manner quite similar to key extraction methods based on time-domain channel variations [38]. An example of this approach is presented in [39], where authors utilized the randomness of channel responses of individual OFDM subcarriers for

efficient key generation method.

In the key generation approaches when a single link cannot generate high secret key rates, a suggested approach is to consider the exploitation of spatial domain for key generation. The space domain approach incorporates multiple antennas and relays for generating secret keys. In fact, multi-antenna techniques of secret key generation and agreement of transceivers greatly improve the channel's randomness [18, 40]. As an example, the authors in [40] investigated multi-antenna systems for key generation in real-time by using RSSI along with multi-level quantization at each antenna. Similarly, in [18], the authors presented a practical key generation method involving channel quantization with singular value decomposition. This particular method can efficiently boost the generated secret key in MIMO systems. Relays are also important components that can be used in the space domain for PLS based key generation [41]. The relays can improve the rate as well as the randomness of the key by providing an alternate path. For example, [42] presents a secret key generation approach that exploits multiple trusted relays. Likewise, [43] proposes a smart scheme for improving the key generation process by employing multiple untrusted relays.

2.4.4.3 Learned Lessons

It should be noted that the above-mentioned studies dealing with the key generation are only concerned with the extraction of high key rates while keeping the randomness of the key. There is another direction related to the application of key at the PHY in which pre-shared keys are used at the legitimate nodes for PHY-encryption (PLE). More specifically, PLE involves the application of key on a symbol level basis. Other than that, pre-shared keys can be helpful in creating: 1) non-linear power modulation that takes advantage of the characteristics of power amplifiers, 2) interfering signals to covert the transmitted symbols, 3) artificial inter-symbol-interference, or 4) suppression or concealing of different features of OFDM waveform.

In should be noted that the key generation schemes based on the channel do not

offer full-fledge PLS since the extracted key applied at the upper layers (similar to other conventional encryption schemes) may be easier to crack using a simple brute force attacks. Likewise, PLE schemes are also considered to provide partial PLS because the problems involving key distribution and management remain, especially if the keys are being shared between the communicating parties. Thus, combining these two approaches into one scheme addresses not only PLS concerns but also solves the issue related to key distribution and management.

The reader should be aware that extracting keys with high rates comes with its own set of challenges, particularly in LOS or poor scattering environments, where there is a lack of variations in the channel as a result of long coherence time. Few studies in the literature have recently addressed these challenges and have proposed the use of randomized beamforming along with diversity to create a virtual random channel or by exploiting artificial interference to extract high secret key rates with good entropy regardless of variations of the channel [12].

2.5 PHY-Authentication Against Spoofing Attacks

This section presents details about the spoofing attacks and their solutions. In a spoofing attack, the control of the communication channel between the legitimate parties is taken by a spoofer. The spoofer can replace, modify, and intercept the messages that are being transmitted between legitimate parties. Moreover, spoofer can also launch a primary user emulation attack (PUEA) and spectrum sensing data falsification (SSDF) attacks in CR to degrade its throughput performance. In the SSDF attack, an illegitimate node provides false sensing information to degrade the performance of the collaborative spectrum sensing approach. On the other hand, PUEA is based on emulating the characteristics of the PU transmission to deceive the SUs about spectrum occupancy. Furthermore, a spoofer can also attack the global positioning system (GPS) receiver by transmitting a fake GPS signal to confuse drones, cars, sailors, etc. In order to protect

wireless communication from a spoofing attack, one of the effective solutions is to use an efficient authentication method.

Authentication is a process that is used to distinguish between authorized and unauthorized nodes. Conventionally, it is handled by cryptography-based approaches. However, these approaches suffer from many critical challenges over the dynamic wireless heterogeneous network, as explained in section 2.1 of this chapter. In order to solve these issues, PHY-authentication can be exploited to validate different nodes. The popular types of PHY-authentication include wireless channel-based authentication and authentication based analog front-end (AFE) imperfections (or RF front-end imperfections) of wireless transceivers [44], as presented in Figure 2.13.

Compared to the conventional cryptography-based approaches, it is extremely difficult to impersonate the PHY-authentication because of their direct relationship with the communication devices and the propagation environment. Moreover, PHY-authentication can be done without demodulating the signal, which can avoid the waste of resources needed for the signal processing of unintended transmission. Furthermore, estimation and compensation techniques of device imperfection and channel are inherent parts of the communication system for enhancing the performance of reception. Hence, no additional security overhead incur in order to accomplish PHY-authentication.

2.5.1 Channel-based PHY-Authentication

This type of authentication is based on exploiting radiometric characteristics of the environment between transceiver pairs such as the RSSI, CSI, direction of arrival (DoA), round trip time (RTT), etc. These features related to the channel can be used to distinguish between authorized and unauthorized nodes.[4] In channel-based authentication, pilot signals are used to estimate the channel in the first step. Afterward, hypothesis testing is done to analyze whether the

[4]The techniques mentioned in section 2.4.4 are applicable for PHY-authentication also.

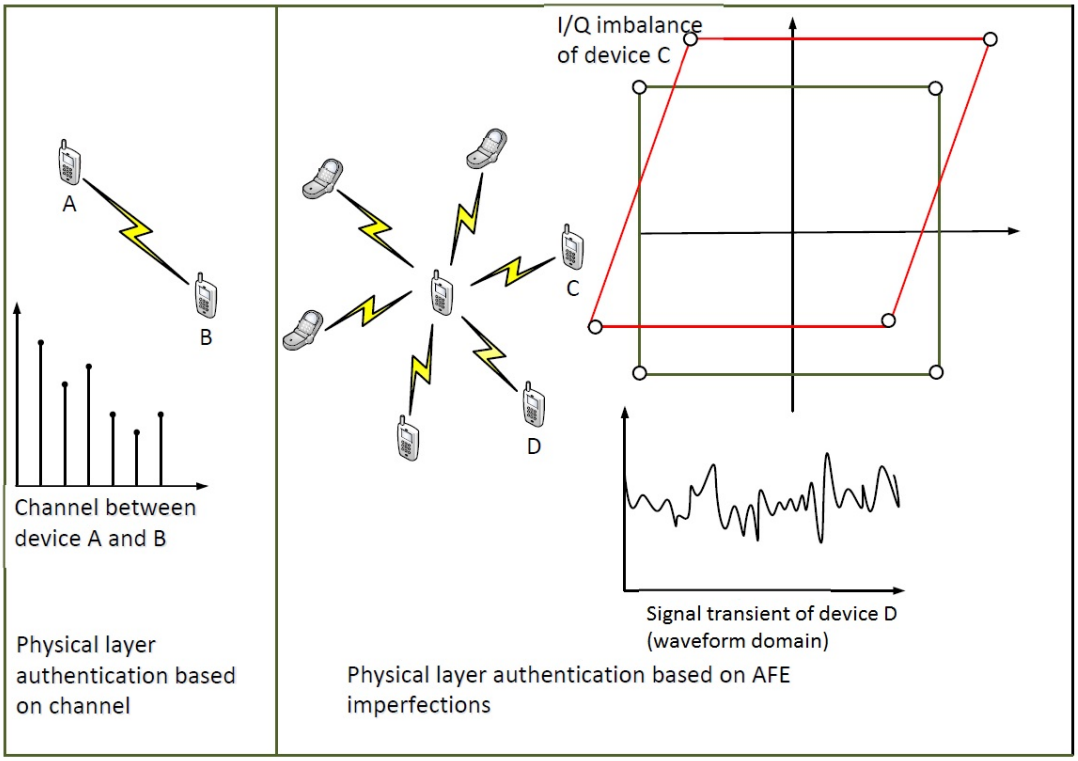


Fig. 2.13: Basic illustration for channel-based authentication versus AFE-based authentication.

current communication attempts are done by the same node which attempted earlier. Figure 2.14 presents a basic system model for PHY-authentication that includes Alice, Bob, and Impersonator. It is assumed that Bob first stores the CSI of Alice ($\mathbf{h}_{AB}$). Afterward, Bob can confirm the authenticity of Alice based on the noisy measured version of the channel ($\mathbf{h}_t$) by using a simple hypothesis test, as given by:

$$\boldsymbol{y} = \begin{cases} \mathcal{H}_0 : \mathbf{h}_t = \mathbf{h}_{AB}, \\ \mathcal{H}_1 : \mathbf{h}_t \neq \mathbf{h}_{AB}, \end{cases} \tag{2.8}$$

where hypothesis, $\mathcal{H}_0$, means null hypothesis, and it shows that the terminal is authorized node, while hypothesis, $\mathcal{H}_1$, means an alternative hypothesis, which shows that claimant is an unauthorized node. CSI based authentication can also be done using machine learning. For example, the authentication algorithm in [45] exploits a linear Fisher discriminant analysis and support vector machine for training the hypothesis test of cyclic feature vectors of CSI.

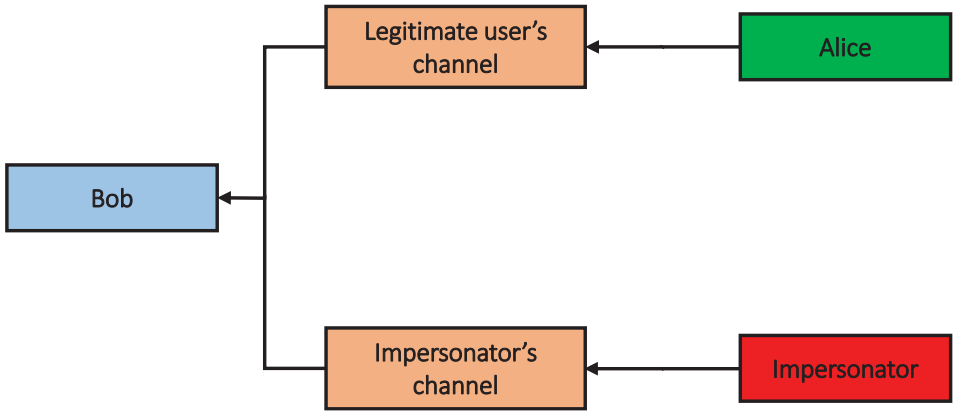


Fig. 2.14: Basic PHY-authentication model that includes Alice, Bob, and Impersonator. Bob stores the CSI between Alice and Bob and it can confirm the authentication of Alice while protecting herself from the Impersonator that is trying to launch spoofing attacks.

2.5.2 AFE-based PHY-Authentication

AFE imperfections, which are relatively more stable than channel-based characteristics, can also be explored for PHY-authentication. The fabrication of the analog components process introduces these inevitable variations (AFE imperfections). Many device-specific characteristics have been exploited for PHY-authentication including carrier frequency offset (CFO), in-phase and quadrature imbalance (IQI), power amplifier characteristics, digital-to-analog converter characteristics, etc. The core of AFE-based authentication includes signal pre-processing, feature extraction, and selection of an appropriate classifier to be trained based on extracted features. Figure 2.15 presents the basic illustration for AFE-based authentication based on machine learning. It includes a system database module that contains a training fingerprint of each enrolled device. This training data is used to train the machine. After classifier training, the testing stage presents the run-time operation of the authentication algorithm. For each incoming test signal, AFE-based feature is extracted after pre-processing of this signal and the feature vector is obtained. Afterward, it is fed into a learned classifier to determine the authenticity of the claiming node. In [46], the author used the Bayesian classifier for frequency, amplitude, and phase recognition. On the

other hand, authors exploit a multi-discriminant classifier to perform one-to-one device verification processes and one-to-many device classifications.

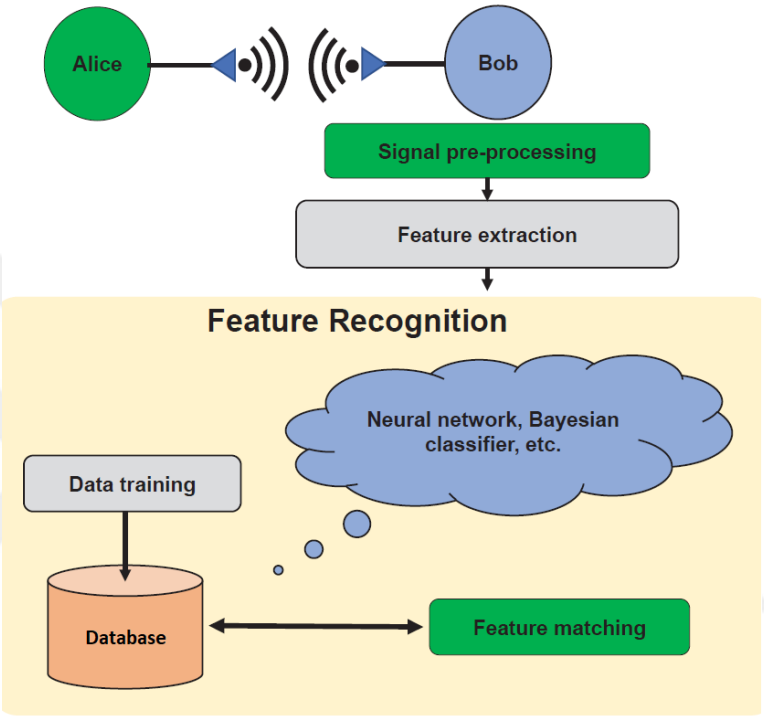


Fig. 2.15: AFE-based authentication scheme using machine learning, which includes signal pre-processing, feature extraction, and feature recognition for authentication.

2.6 Wireless Jamming Attacks and Countermeasures

A jamming attack can be launched by emitting an unwanted radio signal to interrupt the transmission between a legitimate node pair. The intended jammer wants to jam either the transmission or the reception of legitimate wireless communication as presented in Figure 2.16.

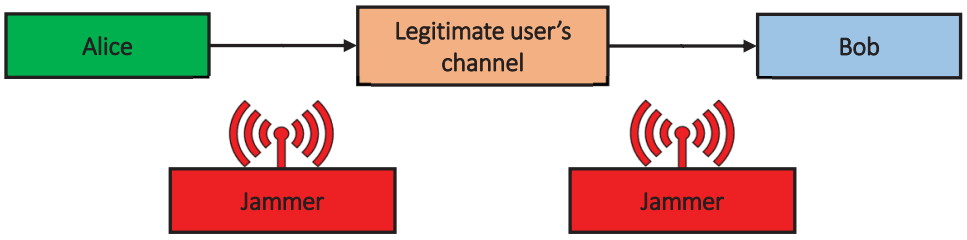


Fig. 2.16: A basic illustration of jamming attacks, where jammer wants to jam either the transmission or the reception of legitimate wireless communication.

2.6.1 Wireless Jamming Attacks: A Brief Summary

The categorization of these jammers based on jamming attacks are as follows:

- A constant jammer, that transmits the jamming signal continuously.
- An intermittent jammer, that transmits the jamming signal periodically.
- A reactive jammer, that transmits only when the legitimate user is active.
- An adaptive jammer, where a jamming signal is tailored to the level of received power at the legitimate receiver.
- An intelligent jammer, who exploits the upper layer protocols to block legitimate user transmission.

2.6.2 Wireless jamming Attacks, Detection, and Solutions

This subsection presents the details about different jamming attacks, their detection methods, and techniques for their countermeasures.

2.6.2.1 Constant Jammer

Constant jammer disrupts legitimate user communication by constantly sending the jamming signal over the shared medium. This constant jamming signal affects

the legitimate transmission in two ways: 1) firstly, because of the transmission of the constant jamming signal, the legitimate transmitter finds the channel always busy, and thus it prevents the legitimate transmitter to access the channel, 2) secondly, it increases the interference and noise to delimit the signal reception quality at the legitimate receiver. Hence, the legitimate communication can be jammed in these two ways regardless of the type of wireless system. However, the constant transmission of jamming signals makes the constant jammer energy-inefficient.

Detection and solution: For the detection of the constant jammer, there are different statistical tests that are based on received signal strength (RSS), carrier sensing time (CST), PER, etc. The RSS detector computed the energy of the received signal and compare it with the predefined threshold value of energy to decide whether constant jammer is present or absent. Thus, the computed energy of the received signal confirms the presence of a jammer on the wireless channel. The constant presence of a jamming signal over the wireless channel may result in high CST, and thus this information can be used for jammer detection. Furthermore, legitimate communication is adversely affected because of jamming, which results in the degradation of PER performance. Therefore, PER can also be used as a parameter to detect the presence of jamming signals. After the successful detection of the jammer, it is required to defend the legitimate transmission against jamming attacks. Frequency hopping is a classical anti-jamming technique that defends against jamming attacks by rapidly changing the carrier frequency with the help of a pseudo-random sequence. Frequency hopping can either be proactive or reactive. In the former case, the transmitter proactively performs pseudo-random channel switching regardless of the presence or absence of the jammer. In the latter case, frequency hopping is performed by switching to a different channel only when the jammer is present. Thus, proactive hopping does not require the detection of the jammer. It should be noted that frequency hopping is resilient against jamming attacks as long as the jammer does not know the pseudo-random hopping patterns. Currently, cryptography-based techniques are employed for the secure generation of pseudo-random hopping patterns. However, the secret key can also be generated by using PHY-characteristics of channel

and AFE imperfection.

2.6.2.2 Intermittent Jammer

Intermittent jammer transmits a jamming signal periodically to interfere with legitimate communication. It sends a jamming signal for a certain time and then it becomes inactive. Hence, compared to constant jamming, energy consumption is reduced. Therefore, from the perspective of energy-constrained scenarios, intermittent jamming is preferred over constant jamming. However, jammer's performance can have a trade-off between jamming effectiveness and energy efficiency by optimization of the transmit time and inactive span. Particularly, an increase in the inactive span improves energy efficiency at the cost of jamming performance degradation.

Detection and solution: For the detection of the intermittent jammer, the same statistical measurements can be used as that of constant jammer detection. Moreover, reactive and proactive frequency hopping could be effective solutions to protect legitimate communication from such jamming attacks.

2.6.2.3 Reactive Jammer

Reactive jammer senses the legitimate user transmission on wireless channel and when it found that the legitimate user is active, it starts transmitting the jamming signal to disturb the legitimate transmission. A reactive jammer's performance depends on its sensing and successful detection of the legitimate user. In scenarios where fast fading and shadowing effects dominate, the detection of the legitimate signal becomes weak, and thus the jammer is unable to detect the legitimate transmissions and is ineffective in such scenarios. However, it is more energy-efficient compared to intermittent and constant jammers.

Detection and solution: The reactive jammer only corrupts the reception

without affecting the legitimate transmitter activity to access the wireless channel. Hence, CST becomes ineffective for the detection of the reactive jammer. However, RSS and PER based detection can be used to detect such jammer because an abnormal increase in RSS and PER depicts the presence of a reactive jammer. An effective solution to defend the legitimate user against reactive jammer is to assist the legitimate user in becoming undetectable. Direct-sequence spread spectrum (DSSS) technique spreads the signal over a wide frequency band, and thus the signal power spectral density is low. In this way, the reactive jammer is unable to track the legitimate traffic activity and it can not corrupt the legitimate transmission. Classical frequency hopping can also work against the reactive jammer if the hopping rate is higher than the jammer's reaction.

2.6.2.4 Adaptive jammer

This jammer can adjust its jamming power to any specified power level to disturb the legitimate transmission. If the channel spanning between transmitter and receiver is good and signal arriving at the legitimate receiver is strong, then adaptive jammer increases its jamming power to efficiently corrupt the legitimate reception. On the other hand, if the channel is having deep fades and a legitimate receiver is not able to decode its received signal, then adaptive jammer may not send a jamming signal at all. While comparing with the constant, intermittent, and reactive jammers, the adaptive jammer is the most energy-efficient one. Moreover, as per observations, the adaptive jammer must have the prior knowledge of signal strength of the legitimate receiver for adapting its jamming power. However, it is a challenging task to obtain a priori knowledge of signal strength in practice, since the main channel's strength varies in time and is unknown to the jammer. This limits the application of the adaptive jammer in practical wireless systems.

Detection and solution: Due to the adaptive power control mechanism of an adaptive jammer, it is task challenging to detect it. Joint detection based on RSS and PER can be performed for the efficient detection of such jammer. If the value of both RSS and PER is unexpectedly high, it indicates the presence of

an adaptive jammer. More specifically, the presence of adaptive jammer causes high RSS and also causes a high PER. Another case is high RSS and low PER, which indicates a reliable legitimate transmission among legitimate transmitter and receiver. In order to defend against adaptive jammer, an effective solution is to evade the adversary. For example, in [47], the authors proposed a pair of evasion methods to defend against the adaptive jamming attacks that include channel surfing and spatial retreating solutions. Specifically, in channel surfing, the legitimate transmitter and receiver are allowed to change their jammed channel to a new channel. On the other hand, the spatial retreating technique enables a jammed wireless node to escape by moving away from the jamming area.

2.6.2.5 Intelligent Jammer

The jamming attacks discussed above are based on the PHY and do not consider the upper layers protocol specifications. On the other hand, an intelligent jammer exploits the vulnerabilities in the upper-layer protocols to interrupt and jam the critical control packets in the network. In order to block the legitimate communications between the source node and the AP, an intelligent jammer can simply corrupt the request-to-send (RTS) or clear-to-send (CTS) control frames, rather than data packets, which minimizes its energy consumption. There are several intelligent jamming attacks such as RTS jammer, CTS jammer, ACK jammer, etc. An RTS jammer senses the channel to be idle for a specified time period and transmits a jamming signal to disrupt a possible RTS packet. Contrastly, a CTS jammer attempts to detect the presence of an RTS frame, and upon detecting the RTS arrival, it waits for the RTS period plus a specified time interval before sending a jamming pulse for disrupting the CTS frame. The CTS jamming strategy will results in zero throughput for the legitimate transmission, since no data packets will be transmitted by the source node without successfully receiving a CTS frame. Similar to the CTS jamming, an ACK jammer also senses the wireless medium, and upon detecting the presence of a packet, it waits for a certain time interval, and then jams the wireless channel, leading to the corruption of an ACK frame. If the source node constantly fails to receive the ACK, it will finally

give up transmitting data packets to the AP.

Detection and solution: The above-mentioned jammers can be detected by tracking the traffic of MAC control packets to check abnormal events and behaviors in terms of sending or receiving the RTS, CTS, and ACK. In order to defend against such attacks, a protocol hopping approach can be used [48]. This approach allows legitimate nodes to hop between different available protocol parameters to ensure reliable communication even in the presence of such jammer. Similarly, a game-theoretic framework to defend against such jammer is proposed in [48], which is based on modeling the interactions between an intelligent jammer and the protocol functions.

Chapter 3

Secret Key Generation Using Channel Quantization with SVD for Reciprocal MIMO Channels

3.1 Introduction

Due to the broadcast nature of wireless signals, the security of wireless devices is becoming more challenging than before. Traditional security techniques are mainly based on cryptographic keys [49] to fulfill the security requirements [50]. However, key establishment, management and distribution processes in wireless networks, are challenging, especially with current and future heterogeneous and de-centralized networks. Recently, physical layer security has drawn great research interest because of its capability in eliminating the requirement of an authenticated communication channel, to manage and distribute keys, by using channel and noise measurement as a source of randomness to generate secret keys [50], [51].

In physical layer-based key generation, the transmitter and receiver extract

random sequences, called secret keys, from the random variations of the reciprocal wireless channel between them, and then use them to encrypt and decrypt the data by performing similar processing at their sides [52], [53]. The fundamental theoretical work behind this direction can be traced back to [54], which is very similar to the work independently done in [55], [56]. The secret key generation analysis made in [54], was extended to account for the presence of an active eavesdropper in [57] [58] [59]. In [60], researchers proposed a technique that uses the short term reciprocity of the radio channel to secure information, in which, the exchange of information does not require the availability of a common secure key between two users since the phase of the fading coefficients are used as a secret key. The proposed technique in [60] can also be used for cryptographic key agreement between two users. In [61], a technique, which directly quantizes the complex channel coefficients, was suggested. In [62], discretizing the extracted coefficients of some practical and standardized multipath components, was investigated. In [63], level crossing rates of the fading processes are exploited for key generation. In [64], channel estimates are used as correlated random variable for information reconciliation. Quantization of channel phases to generate longer keys for a multi-tone communication system was studied in [65] [66] [67]. On the other hand, the authors of [68], [69] used time-varying frequency characteristics of OFDM wireless systems to explore channel based key generation and key agreement.

Multiple-antenna based devices are capable of significantly increasing the randomness of channel, which can be used for secret key generation and agreement. Recently, multiple antenna links and the corresponding secrecy and secret key rates are studied in [70], [71]. In [72], the secret key rate for the basic source model with a MIMO channel was studied. In [73], a practical multiple-antenna based key generation technique is presented, in which the randomness is extracted from the measured received signal strength indicator (RSSI). It was shown that the increase in the number of antennas at Eve could not infer more information to her about the secret keys generated from the main channel. In [74], the author proposed two practical key generation techniques for the MIMO-OFDM systems. The first is based on using precoding matrix indicator (PMI) for secret key generation, while the second matrix is based on channel quantization for increasing the

length of the secret key. In RSSI and channel quantization-based key generation techniques [71], the length of the generated key is not only affected by the channel randomness, but also by the quantization method applied on the estimated channel coefficients.

In this work, we develop and propose a key generation method based on channel quantization with SVD (CQSVD), for increasing the generated key length in MIMO systems. In specific, the amplitudes and phases of the complex MIMO channel coefficients, are quantized using the proposed CQSVD method. By using this method, it is shown that a key vector of length $2M^3$ can be generated from a block fading $M \times M$ MIMO channel. To achieve key renewal process, the generated key vector can be updated over each fading block or after several blocks. Moreover, in this work, encryption is performed on a symbol level basis rather than bit level-basis to provide more secure communication, since in this case brute force attack cannot easily be performed on the application layer without using specific devices to capture the data symbols. The obtained results prove that the employment of such method can significantly increase the key length, without causing high key mismatch probability or breaking its uniformity and randomness. Additionally, since the operation of this method highly depends on the channel, the key performance is tested against the effect of imperfect channel estimation and imperfect reciprocity.

The rest of the paper is organized as follows. In Section II, the system model is presented. Then, the proposed method is explained in Section III. In Section IV, the simulation results are discussed, while the conclusion is drafted in Section V.

3.2 System Model and Preliminaries

We consider a spatial multiplexing MIMO communication system model as presented in Fig. 3.1. In particular, a legitimate source (Alice) and a legitimate user (Bob), that are equipped with multiple antennas denoted by M_t and M_r, respectively, want to generate a shared secret key vector by using the channel related information, i.e., amplitude and phase. The antenna spacing at each terminal is

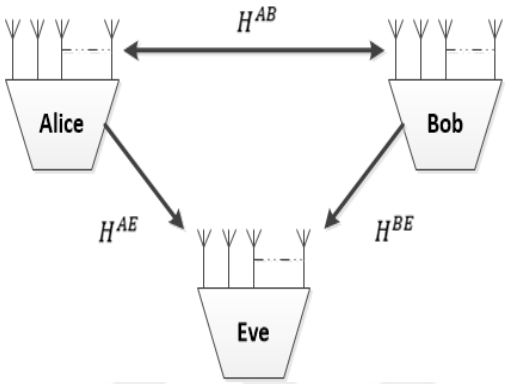


Fig. 3.1: The wireless communications scenario considered in this work.

at least have wavelength ($\frac{\lambda}{2}$) to provide sufficiently de-correlated signals. Also, there is a passive adversary, Eve, who tries to eavesdrop on the communication between Alice and Bob. Eve is equipped with multiple antennas (M_e) and can listen to all the communication between Alice and Bob, and she also knows the key extraction algorithm. We also assume that Eve cannot be very close to legitimate nodes, i.e., Eve's distance to legitimate nodes cannot be less than few multiples of the wavelength [75]. This will ensure that Bob and Eve experience independent channel realizations [54]. Under these assumptions, Alice first transmits a reference signal to Bob for channel estimation and then Bob sends back a reference signal to Alice and after that they apply CQSVD method, which will be explained in detail in the next section. After that, Alice applies symbol level encryption on the transmitted data symbol vector $\mathbf{x_n} \in C^{M_t \times 1}$ using a phase randomization (PR) vector, made from the extracted key. Alice then transmits the resulting encrypted data symbol vector $\mathbf{x} \in C^{M_t \times 1}$ to Bob. The baseband received signal at Bob's side in a matrix form is given by

$$\mathbf{y^b} = \sqrt{\frac{E_x}{M_t}}\mathbf{H^b x} + \mathbf{z^b} \tag{3.1}$$

where, E_x is the symbol energy, M_t is the number of transmit antennas, $\mathbf{H^b} \in C^{[M_r \times M_t]}$ and $\mathbf{z_b} \in C^{M_r \times 1}$ are the complex channel response and the zero-mean complex additive white Gaussian noise (AWGN) of Bob's channel, respectively. The baseband received signal at Eve's side in matrix form is given by

$$\mathbf{y^e} = \sqrt{\frac{E_x}{M_t}}\mathbf{H^e x} + \mathbf{z^e} \tag{3.2}$$

Where $\mathbf{H^e}$ and $\mathbf{z^e}$ are the complex channel response, and AWGN of the Eve's channel, respectively. It should be noted that in this system we assume that each antenna (independent of the others) experiences a one-tap Rayleigh fading channel with constant channel gain over one packet length, but independent and identically distributed (i.i.d) from one packet to another. Accordingly, the minimum mean square error (MMSE) signal detection at Bob's and Eve's side is given by [76] as follows

$$\hat{\mathbf{x}}_{MMSE}^{b/e} = \hat{\mathbf{W}}_{MMSE}^{b/e}\mathbf{y^{b/e}} \tag{3.3}$$

$$= (\mathbf{H^{*b/e}H^{b/e}} + \sigma_z^2\mathbf{I})^{-1}\mathbf{H^{*b/e}y^{b/e}} \tag{3.4}$$

$$= \hat{\mathbf{x}}_{b/e} + (\mathbf{H^{*b/e}H^{b/e}} + \sigma_z^2\mathbf{I})^{-1}\mathbf{H^{*b/e}z^{b/e}}. \tag{3.5}$$

Where $\mathbf{H}^*$ is the hermitian transpose of the channel, while $\hat{\mathbf{x}}_{MMSE}$ is the estimated signal by using MMSE detection method. After this step, the receiver, Bob will apply symbol based decryption to get the original version of the signal, while Eve will receive a degraded version of the signal.

3.3 Proposed CQSVD Method

In this section, we explain our proposed CQSVD method to generate a PR vector for symbol level encryption as presented in Fig. 3.2. Under the assumption of channel reciprocity, $H^{AB} = (H^{BA})^T$, where H^{AB} and H^{BA} are the channels between Alice and Bob and between Bob and Alice, respectively, and $(.)^T$ stands for the transposition. In this way, Alice and Bob are able to compute similar information for key generation, but Eve is unable to generate similar key [71]. Hence, channels between Alice and Eve H^{AE} and between Bob and Eve H^{BE} are independent to H^{AB} and H^{BA}, respectively. To generate shared secret key vector (PR vector) in the multiple antenna system by using CQSVD method, Alice and Bob perform the following main steps:

1. Estimation of the complex channel coefficient's matrix.
2. Decomposition of the channel matrix.

3. Generation of random matrices.

4. Reshaping to generate PR vector.

Each of the main step has further small sub-steps. The detail of the main steps and their sub-steps is as follows:

3.3.1 Estimation of the Complex Channel Coefficient's Matrix

1. In the first step, Alice sends a reference signal **ref** $\in C^{M_t \times 1}$ to Bob for channel estimation.

2. Bob estimates the channel $H^{AB} \in C^{[M_r \times M_t]}$ and sends a reference signal to Alice (within coherence time).

3. Alice also estimates the channel $H^{BA} \in C^{[M_r \times M_t]}$ from reference signal.

3.3.2 Decomposition of Channel Matrix

After estimating the channel matrix {H} at both Alice and Bob, each node will do the following steps:

1. Finding magnitudes and phases of the matrix {H}.

2. In order to generate PR vector for encryption, the channel magnitude matrix and phase matrix are decomposed by using simple SVD or alternative SVD, and then step (C) and (D) are performed. Firstly, we will explain matrix decomposition by using simple SVD and then by using alternative SVD. In linear algebra, SVD states that a rectangular matrix $\mathbf{G} \in C^{[M_r \times M_t]}$ can be factorized into product of three matrices [77] as follows:

$$SVD\{\mathbf{G}\} = \mathbf{USV^T}, \tag{3.6}$$

where $\mathbf{S}$ is a diagonal matrix, $\mathbf{U}$ is a unitary matrix and $\mathbf{V^T}$ is the transpose of another unitary matrix. Firstly, We apply simple form of SVD on the channel's magnitude and phase matrix and then implement step (C) and (D) to generate PR vector for encryption. Since applying SVD on the channel's magnitude and phase matrix gives 6 matrices, each has size of $(M \times M)$, where four of them are unitary matrices, while the other two are diagonal matrices, the total length of resulting PR vector by using simple SVD is $4M^2 + 2M$ as presented in Fig. 3.2. However, the length can further be increased by using an alternative form of SVD as presented in Fig. 3.2. The alternative form of SVD can be used to decompose any matrix $\mathbf{G} \in C^{[M_r \times M_t]}$ into a weighted, ordered sum of M separable matrices [77] as follows:

$$\mathbf{G} = \sum_{i=1}^{M} \mathbf{A_i} = \sum_{i=1}^{M} \sigma_\mathbf{i} \mathbf{u_i} \otimes \mathbf{v_i} \tag{3.7}$$

where $\mathbf{u_i}$ and $\mathbf{v_i}$ are the i^{th} columns of the corresponding SVD matrices $\mathbf{U}$ and $\mathbf{V}$, respectively, and $\sigma_\mathbf{i}$ is the i^{th} ordered singular values from $\mathbf{S}$, and each $\mathbf{A_i}$ is $M \times M$ matrix. Note that the number of non-zero σ_i is exactly the rank of the matrix. So, by using this alternative form of SVD both the channel amplitude matrix as well as channel phase matrix are decomposed into M matrices, each of which contains $M \times M$ elements. In this way, we get total $2M$ quantized matrices per MIMO channel observation, and from which PR vector of length $2M^3$ can be obtained by applying steps (C) and (D), which is much more longer than the length of PR vector by simple SVD case that is $4M^2 + 2M$ as presented in Fig. 3.2. So, we prefer to use alternative form of SVD in CQSVD method.

3.3.3 Generation of PR Matrices

After getting matrices from alternate form of SVD, both Alice and Bob will apply the following procedure on each matrix to generate PR matrices.

1. Take the mean p of each matrix and compare it with every entry of matrix

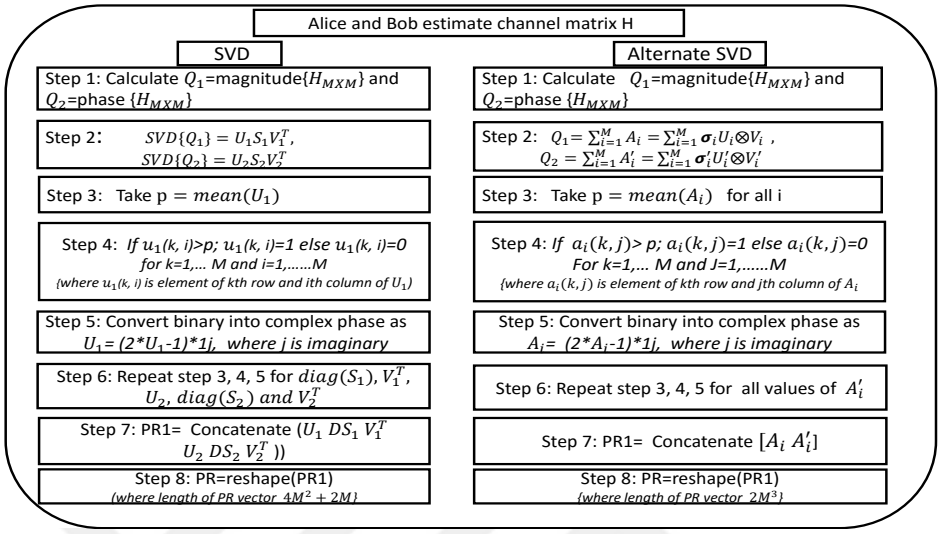


Fig. 3.2: SVD and Alternate SVD based channel quantization method.

A. If the value of any element is greater than p assign one to that index, else assign zero. With this procedure the resultant matrix will contain random values of 1's and 0's.

2. As explained earlier that our scheme is based on symbol level encryption, so we have to convert 1's and 0's into phases. We achieve this task by multiplying each element in the matrix by 2, subtracting 1 and then multiplying by "j", $(2 \times A - 1) \times 1j$, where j is an imaginary number. The resultant matrix is called PR matrix. We apply the above mentioned procedure on each of the remaining matrices.

3.3.4 Reshaping to Generate PR Vector

1. Finally, we concatenate these PR matrices into one vector called PR vector of length $2M^3$.

2. In the literature of channel-based secret key generation methods, data encryption is usually applied on a bit level basis. However, in our method, the extracted secret key is applied on a symbol level basis as it is composed of random phases instead of random bits. This feature increases the security

level against eavesdroppers as compared to bit level encryption.

After generating PR vector, Alice generates a signal, modulates it and divides modulated symbols into M_t streams, in such a way that each frame contains $2M^3$ symbols, and then encrypt these symbols by multiplying each symbol with an element of PR vector, for example, encryption of any symbol x_n is given by

$$r_k = Ae_k^{\phi} \tag{3.8}$$

$$x = x_n r_k \tag{3.9}$$

where r_k is an element in PR vector, $A = 1$ and $\phi_k \in j, -j$ are amplitude and phase of r_k, respectively, x_n is the original data symbol and x is the encrypted symbol. The process of decryption x is performed at Bob by dividing output of MMSE detector by r_k.

$$\hat{x_n} = \hat{x}/r_k = Ae_k^{\phi} \tag{3.10}$$

In this way, Bob will get the original symbol. It is mentioned in [71] that theoretical results predict M^2 growth of key generation rates, without channel quantization, for a MIMO system. However, key of length longer than M^2 can be generated by using different method of quantization [71]. Hence, by using SVD, at high SNR, we can generate a key vector of length $4M^2 + 2M$. This length can further be enlarged by using alternate SVD, which can generate a key vector of length $2M^3$. It should be emphasized that unlike the quantization techniques in [53], [65] and [71], which require public sharing of information about the used quantization level, the proposed CQSVD method does not require sending any public messages about quantization. To reduce the key mismatch probability between the estimated keys and increase its robustness, we propose using powerful estimators, whose training data symbols are long enough and have sufficient power.

It should be noted that in our algorithm due to the comparison with the mean in the process of key generation (Step C), the key is expected to be uniform and it will be shown in the next section. The randomness of our key is verified by using

Run test function for randomness provided by MATLAB Statistics Toolbox as h=runstest(**r**), where **r** is our generated key vector (Step C). This function returns a test decision for the null hypothesis that the values in the data vector **r** come in random order, against the alternative that they do not. The test is based on the number of runs of consecutive values above or below the mean of **r**. The value of result h is 1 if the test rejects the null hypothesis at the 5 % significance level, or the value is 0 otherwise [78], where $h = 0$ means random and $h = 1$ means not random. In our case, several tests are carried out for different channel and all of them have given a result of zero, which means the key is random.

3.4 Simulation Results

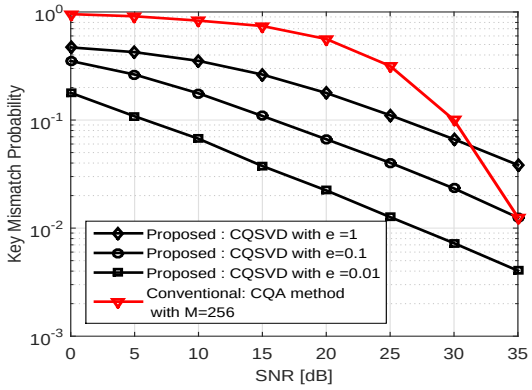


Fig. 3.3: Secret key mismatch probability (key error rate) under imperfect channel estimation and imperfect channel reciprocity.

In this section, simulation results are presented to analyze the effectiveness of the proposed secret key generation scheme based on CQSVD method. In order to fully assess the performance of the generated key, two main metrics, which reflect the effect of the estimated channel and the adopted quantization method, are evaluated. These metrics include key mismatch probability (error rate) and key rate (efficiency) per matrix of MIMO channel coefficients. Moreover, the CQSVD is compared with the state of the art channel quantization alternating (CQA) method for key generation from reciprocal MIMO channels [79]. In all the simulations, imperfect channel estimation and imperfect channel reciprocity due

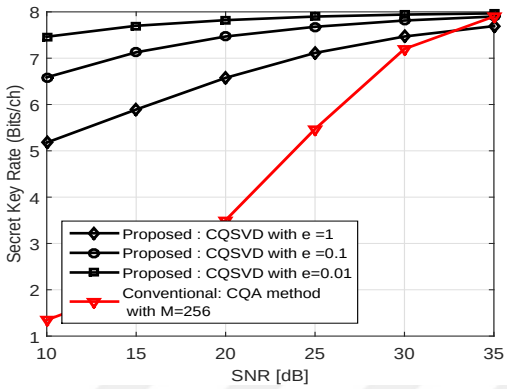


Fig. 3.4: Secret key rate (efficiency= Bits/channel coefficient) vs SNR, under imperfect channel estimation and imperfect channel reciprocity.

to possible realistic synchronization, interference and noise errors are taken into account. This is performed by introducing intentional independent estimation errors to both Alice and Bob. Thus, the estimated erroneous channels at Alice and Bob can be modeled as $\hat{\mathbf{H}}^{\mathbf{a}} = \mathbf{H} + \mathbf{\Delta H}^{\mathbf{a}}$ and $\hat{\mathbf{H}}^{\mathbf{b}} = \mathbf{H} + \mathbf{\Delta H}^{\mathbf{b}}$, respectively, where $\mathbf{H}$ is the true channel. $\mathbf{\Delta H}^{\mathbf{a}}$ and $\mathbf{\Delta H}^{\mathbf{b}}$ are modeled as independent complex Gaussian noise vectors with zero mean and error variance $\sigma^{\mathbf{2}} = e \times 10^{\frac{-SNR_{dB}}{10}}$. It should be emphasized that the error variance value of the estimated channel depends on the quality of the adopted estimator, which is highly affected by the length of the training sequence and its power. Thus, three variances with different e's, corresponding to three different estimators, are considered.

Fig. 3.3 shows the key mismatch probability (KMP) between the generated key sequences at Alice and Bob, whose estimated erroneous channels are independent, but have equal variance value since the same estimators are considered at both sides. It is clear that as $\sigma^{\mathbf{2}}$ decreases by reducing e from 1 to 0.01, the KMP of the proposed method (CQSVD) also decreases. Also, it is shown that CQSVD outperforms CQA method with a quantization level Q equals to 256, at SNRs less than 30. It should be mentioned that CQA method can have different Q values. However, for fair comparison, Q=256 is selected for comparison since CQA with Q=256 can generate the same key rate as that of CQSVD at high SNR, as it can be shown in Fig. 3.4 at SNR=35 dB. For more details about CQA, readers can refer to [71]. Fig. 3.4 presents the possible key rate measured in terms of bits per single estimated channel coefficient and is defined as the average identical

number of bits that can be extracted from a single channel coefficient. It is evident from Fig. 3.4 that CQSVD exceeds CQA at low SNRs since the channel quantization process in CQSVD exploits the orthogonality property brought by SVD, instead of sector segmentation process employed by CQA, which is more sensitive to noise than CQSVD. However, at high SNRs, it is noticed that both CQSVD and CQA have the same key rate as both methods become noise-error free. In general, for a block fading MxM MIMO system with M^2 channel degree of freedom (coefficients), the length (L) of the generated key can be defined as $L = M^2(1 - KMP)c$, where $c = 2M$ is the maximum number of generated bits per estimated channel coefficient. Furthermore, the secrecy rate (SR) can be defined as $SR = (1 - KMP)c$. In Fig. 3.5, we show the distribution of the key before conversion into complex phase (Section III, Step C). It is clear that our key vector is approximately uniform. Fig. 3.6 presents the phases of the complex RP vector (Section III, Step D). It is clear that key is approximately random. The randomness is also verified by run test function, provided by MATLAB Statistics Toolbox (2015) (as explained earlier in Section III).

Now, since the proposed scheme implements symbol level encryption by using the generated PR vector, it is of importance to test the effect of the developed technique on data communication. This can be characterized by calculating the BER performance versus SNR [50]. The simulation parameters of the considered spatial multiplexing MIMO system are presented in Table 3.1. In the simulation, in order to check the robustness of the method, both imperfect channel

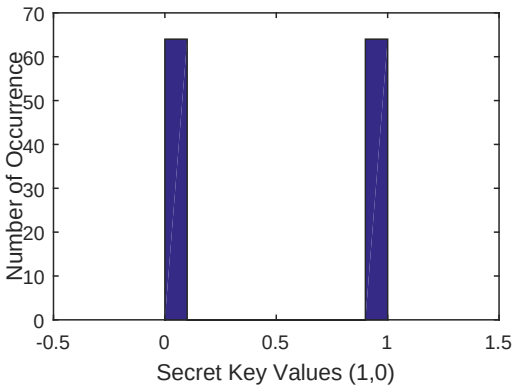


Fig. 3.5: Distribution of elements of PR key vector (step D1) (uniformity).

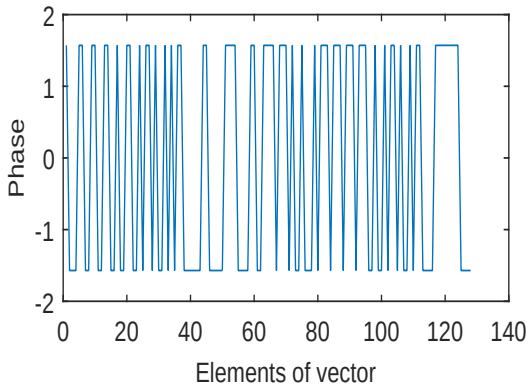


Fig. 3.6: Phase of final PR key vector (randomness).

Table 3.1: Simulation parameters

No of antenna at Tx	4
No of antenna at Rx	4
Block (Packet) length	128
Modulation	4-QAM
No. of Packets/frame	1000
No. of frames	128
Equalization type	MMSE
Fading type	Raleigh fading channel

estimation (ICE) and imperfect channel reciprocity (ICR) are considered at all communication parties [80]. In specific, channel estimation errors are modeled as mentioned before and we will show performance for $e = 0.01$ and $e = 0.001$. Fig. 3.7 presents the effect of employing secret key generation using CQSVD method on the BER performance of the considered spatial multiplexing MIMO system. It is shown that ICE and ICR lead to a small degradation in the BER, due to the mismatch between the generated PR vectors at both sides. It should be noted that the resulting small degradation can be overcome by increasing the training sequence length and its power, where better channel estimation can be obtained.

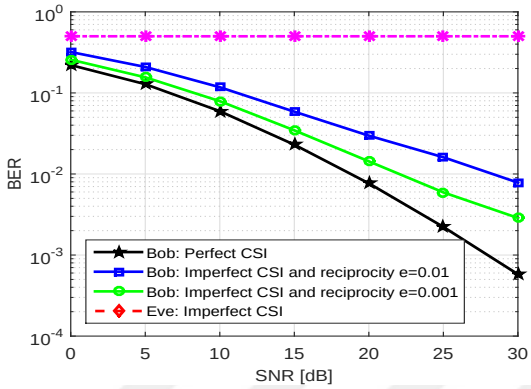


Fig. 3.7: BER performance of RP method with QPSK under imperfect channel estimation and imperfect channel reciprocity.

3.5 Conclusion

This paper has provided a secret key generation method, called CQSVD, which exploits the reciprocity of $M \times M$ MIMO channel. In this method, a phase randomization (PR) key vector for symbol level encryption is generated by applying alternative form of SVD on channel's phase and magnitude matrices. It was shown that for $M \times M$ MIMO channel, a key length of $(2M^3)$ can be generated. Simulations with a simple 4×4 MIMO channel have been presented. The scheme has been analyzed for perfect and imperfect channel estimation as well as for perfect and imperfect channel reciprocity.

Chapter 4

A New Physical Layer Key Generation Dimension: Indices Based Key Generation

4.1 Introduction

The broadcast nature of wireless communication makes it vulnerable to adversarial eavesdropping and intervention. In current wireless networks, to ensure confidentiality, integrity, and authentication of wireless communication, classic encryption-based techniques are employed at the upper layers [12]. However, these techniques may not be suitable for the fifth-generation (5G) and beyond heterogeneous wireless networks because of the complexity of establishment, management, and distribution of secret keys in such networks. In addition, with the development of powerful computing devices, these encryption-based techniques become more susceptible to sophisticated adversaries. In order to solve the problems faced by traditional security techniques, the physical layer key generation provides an efficient complementary solution to both asymmetric and symmetric encryption algorithms. The basic idea is to exploit the channel reciprocity property between communicating nodes as a common source of randomness for secret

key generation. Also, in a rich multi-path scattering environment, an eavesdropper will experience uncorrelated channel measurements if it is half-wavelength apart from legitimate nodes. Thus, Eve cannot extract key bits similar to those extracted by legitimate nodes. Besides, the key generation from channel does not need any infrastructure for its distribution and management [81].

Among many top research areas in physical layer key generation, securing the orthogonal frequency division multiplexing (OFDM) waveform has got much attention [82]. There are several works in the literature proposing different techniques for secret key generation in OFDM based systems. These techniques are based on the exploitation of phases and amplitudes of the channel impulse response (CIR), received signal strength (RSS), and other feedbacks for key generation [35]. The authors in [83] proposed RSS based key generation for the OFDM system in indoor and outdoor environments. In [84], multiple independent phases are quantized to generate secret keys in a multi-tone communication system. On the other hand, authors of [85] studied the secret key generation of an OFDM system based on phase change of the time-varying channel frequency response. In [86], precoding matrix indices along with OFDM subcarriers are exploited to generate secret keys.

One of the main challenges in the channel-based key generation is to increase the secret key length while maintaining the randomness and uniformity of the key. The above-mentioned techniques mainly exploit phases and amplitudes of channel gains or RSS for random and uniform secret key generation. However, all of these methods have certain limitations in terms of secret key generation rate [87]. In order to further enhance the key rate of the conventional key generation methods, in this work, novel key generation methods for multi-carrier systems are proposed. The contributions of the proposed work are as follows:

1. New dimensions of secret key generation for single-input single-output (SISO) multi-carrier communication systems are proposed, where positions/indices of subcarriers corresponding to the largest channel gains are exploited to generate secret key bits along with amplitudes of subcarriers.

Hence, they provide a novel way to enhance the overall key rate of conventional key-based algorithms. The proposed methods are inspired by the concept of OFDM with index-modulation (OFDM-IM) [88]. Particularly, similar to the concept of OFDM-IM, the whole OFDM is divided into subblocks and a subset of subcarriers is selected in each subblock. However, in the proposed algorithms, the subcarriers in each subblock are not selected based on data to convey information as in OFDM-IM but rather selected adaptively based on the positions of largest channel gains in each subblock between legitimate nodes to generate secret keys. Thus, the proposed approaches will enhance the overall key rate of conventional key generation-based algorithms.

2. The proposed approaches are applicable to any multi-carrier system such as OFDM, OFDM-IM [88], and OFDM-SIS [82] [89] for providing confidentiality and authentication against eavesdropping and spoofing attacks, respectively. In addition, the proposed algorithms also have the potential to be explored in other domains such as space, time, and code.

3. In order to get useful insights into the proposed key generation methods different performance metrics such as key mismatch rate (KMR) and key generation rate (KGR) are evaluated. Moreover, in order to check the randomness of generated key bits, a statistical test suite provided by the National Institute of Standards and Technology (NIST) is adopted.

Notations: Matrices are denoted by bold-capital letters, vectors are denoted by bold-small letters. The Hermitian and transpose are represented by $(\cdot)^{\mathrm{H}}$ and $(\cdot)^{\mathrm{T}}$, respectively. $\lfloor . \rfloor$ represents the floor function.

4.2 System Model and the Proposed Algorithm

4.2.1 System Model

The system model is assumed to be single-input single-output (SISO) OFDM wireless system with time division duplexing (TDD), where the legitimate transmitter (Alice) tries to communicate securely with a legitimate receiver (Bob) in the presence of a passive eavesdropper (Eve) as shown in Fig. 4.1. The impulse responses of the channels between Alice-Bob, $\mathbf{h_b}(\mathbf{h_{ab}}) \in \mathbb{C}^{[1\times L]}$, Bob-Alice $\mathbf{h_a}(\mathbf{h_{ba}}) \in \mathbb{C}^{[1\times L]}$, and Alice-Eve, $\mathbf{h_e}(\mathbf{h_{ae}}) \in \mathbb{C}^{[1\times L]}$, are assumed to be slow varying Rayleigh fading channel with L exponentially decaying taps. The property of reciprocity is also adopted, where the channel $\mathbf{h_{ab}}$ can be estimated from $\mathbf{h_{ba}}$. In addition, due to the location and environment differences, both Bob and Eve are assumed to experience independent channels. At the trans-

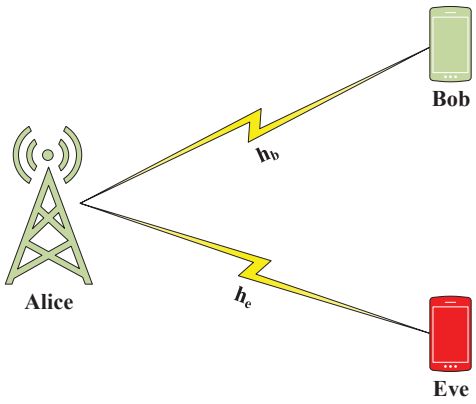


Fig. 4.1: A simplified system model for the considered security algorithm.

mitter, the frequency domain OFDM symbols (pilots) can be represented as $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & \dots & s_{N-1} \end{bmatrix}^{\mathrm{T}} \in \mathbb{C}^{[N\times 1]}$, where N represents the number of frequency domain complex data symbols (pilots). In order to map the pilots symbols to orthogonal subcarriers, the resulting block is passed through an IFFT process $\mathbf{F}^{\mathrm{H}} \in \mathbb{C}^{[N\times N]}$, where $\mathbf{F}$ is the discrete Fourier transform matrix. Afterwards, a cyclic prefix (CP) of length L is inserted by employing the CP appending matrix $\mathbf{C} \in \mathbb{R}^{[(N+L)\times N]}$. Finally, the resultant signal $\mathbf{x}$ is transmitted through the channel, and reaches to both Bob and Eve. Afterward, each of them uses matrix

$\mathbf{D} \in \mathbb{R}^{[N\times(N+L)]}$ to remove CP and then applies FFT process using the matrix $\mathbf{F} \in \mathbb{C}^{[N\times N]}$ to convert the signal into the frequency domain for estimating the channel. The received signal in frequency domain, $\mathbf{y_{b/e}} \in \mathbb{R}^{[N\times 1]}$, at Bob/Eve can be given as

$$\mathbf{y_{b/e}} = \mathbf{FD}\left(\mathbf{H_{b/e}CF}^{\mathrm{H}}\mathbf{s} + \mathbf{z_{b/e}}\right), \tag{4.1}$$

$$= \mathbf{H^{f}_{b/e}s} + \hat{\mathbf{z}}_{\mathbf{b/e}}, \in \mathbb{C}^{[N\times 1]}, \tag{4.2}$$

where vectors $\mathbf{z_{b/e}}$ and $\hat{\mathbf{z}}_{\mathbf{b/e}}$ represent the zero-mean complex additive white Gaussian noise (AWGN) and its Fourier transform, respectively, with variance of $\sigma^2_{b/e}$ at Bob/Eve. On the other hand, $\mathbf{H_{b/e}}(\mathbf{H_{ab/ae}}) \in \mathbb{C}^{[(N+L)\times(N+L)]}$ and $\mathbf{H^{f}_{b/e}} = \mathbf{H^{f}_{ab/ae}} = \mathbf{FDH_{b/e}CF}^{\mathrm{H}} \in \mathbb{C}^{[N\times N]}$ represent the Toeplitz matrix corresponding to the channel impulse response and the diagonal matrix corresponding to the channel frequency response, respectively, with respect to Bob/Eve.

4.2.2 Proposed Algorithms

This section presents the details about the proposed indices based key generation (IKG) and joint key generation (JKG) algorithms.

The basic steps for the IKG algorithm are as follows:

1. In the first step, Alice and Bob send pilot signals, $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & \dots & s_{N-1} \end{bmatrix}^{\mathrm{T}} \in \mathbb{C}^{[N\times 1]}$, to each other within the coherence time of the channel to estimate the channel as explained in subsection 4.2.1. The estimated channel at any node (Alice/Bob) in frequency domain can be represented as $\mathbf{H^{f}} \in \mathbb{C}^{[N\times N]}$.

2. The resultant diagonal channel matrix at any node is multiplied with a random interleaver, $\mathbf{R}$, and the resultant vector can be given as $\mathbf{h_f} = \mathrm{diag}(\mathbf{H^{f}R})$, where $\mathbf{h_f} \in \mathbb{C}^{[N\times 1]}$. Note that the interleaving operation is employed to distribute the deep fades of subchannel uniformly over whole

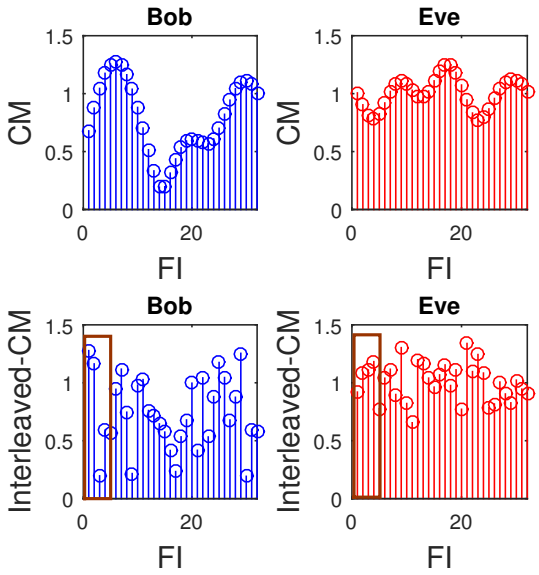


Fig. 4.2: Channel magnitude (CM) versus frequency index (FI) for frequency responses of channel of Bob and Eve (shown in upper part of the figure) alongside their interleaved channels i.e., $\mathbf{H}_{\mathbf{b}}^{\mathbf{f}}\mathbf{R}$ and $\mathbf{H}_{\mathbf{e}}^{\mathbf{f}}\mathbf{R}$ (shown in lower part of the figure) along with IKG algorithm.

OFDM block and make them look random and uncorrelated as presented in Fig. 4.2.

3. Afterwards, the whole $\mathbf{h_f}$ vector is divided into G subblocks with n elements in each subblock ($\mathbf{h}_\beta$), where $\mathbf{h_f} = [\mathbf{h}_1, \ldots, \mathbf{h}_G]$, $\mathbf{h}_\beta = [h_{\beta,1}, \ldots, h_{\beta,n}]$, $G = N/n$ and, $\beta \in \{1, \ldots, G\}$.

4. In the next step, the absolute values of each of subblock's elements are calculated as $|h_{\beta,j}|$, where $h_{\beta,j}$ is the j_{th} element of $\mathbf{h}_\beta$ subblock.

5. Afterwards, m_β number of strongest subcarriers are selected in each of $\mathbf{h}_\beta$ subblock based on the values of $|h_{\beta,j}|$. Finally, their positions/indices are used to generate key bits by using look-up table. The look-up table maps the position of indices to key bits. A look-up table example is presented in Table I for $n = 4$, $m_\beta = 2$. The first column of Table I shows the m_β strongest subcarriers in h_β subblock, the second column shows the position/indices of the strongest subcarriers, and the third column shows the generated key bits corresponding to those indices. The total number of key bits generated

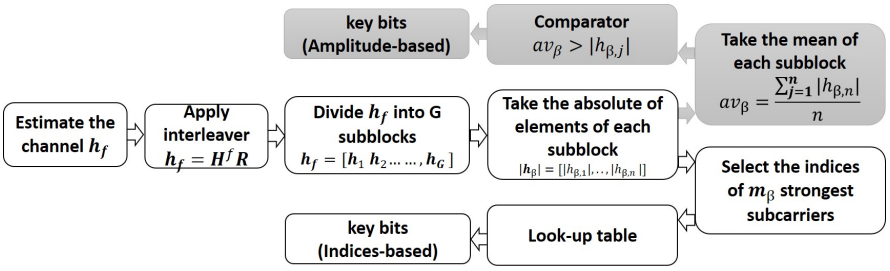


Fig. 4.3: Proposed IKG and JKG algorithms, where IKG includes all blocks except the gray ones while JKG includes all blocks.

in any OFDM block is a function of m_β, n, N, and G that can be given as $G\lfloor \log_2 \binom{n}{m_\beta} \rfloor$.

Table 4.1: Look-up table for IKG algorithm for m=2 bits and n=4

subblocks	Indices	Key bits
$\left[\lvert h_{\beta,1}\rvert\ 0\ 0\ \lvert h_{\beta,4}\rvert\right]$	{1, 4}	[0 0]
$\left[0\ \lvert h_{\beta,2}\rvert\ 0\ \lvert h_{\beta,4}\rvert\right]$	{2, 4}	[0 1]
$\left[\lvert h_{\beta,1}\rvert\ 0\ \lvert h_{\beta,3}\rvert\ 0\ \right]$	{1, 3}	[1 0]
$\left[0\ \lvert h_{\beta,2}\rvert\ \lvert h_{\beta,3}\rvert\ 0\right]$	{2, 3}	[1 1]

In order to further clarify IKG, consider the following example. Lets suppose we have $\mathbf{h_f} \in \mathbb{C}^{[N\times 1]}$, $N = 128$, $m_\beta = 2$, and $n = 4$. Afterwards, $\mathbf{h_f}$ is divided into $G = N/n = 128/4 = 32$ subblocks. In each subblock, $m_\beta = 2$ strongest subcarriers are selected. Afterwards, the positions of these subcarriers for each subblock are mapped to generate key bits by using Table I. The total number of key bits generated by OFDM block is 64 for IKG algorithm. Note that m_β can take any value from the set, $\{1, \dots, n-1\}$, but in this algorithm one of the values from this set is used for all subblocks, $m_\beta = 2$.

In order to further enhance the key rate of IKG, a joint key generation (JKG) approach is suggested. In the JKG approach, bits are generated by using both indices as well as amplitudes of subcarriers. The first four steps $(1, 2, 3, 4)$ of JKG are similar to the IKG algorithm. In the fifth step, firstly, the key bits

are generated from the indices of h_β subblock similar to the fifth step of IKG. Afterwards, the average of absolute values of subblock's element is calculated as follows:

$$av_\beta = \frac{\sum_{j=1}^{n} |h_{\beta,j}|}{n}, \tag{4.3}$$

where $\beta \in \{1, \ldots, G\}$. Finally, each element of h_β subblock is compared with its mean, av_β, to generate secret key bits. For example, if $|h_{\beta,j}| > av_\beta$, 1 is generated as key bit otherwise 0 is generated. Hence, JKG based approach provides a higher key rate by exploiting both indices and amplitudes. For example, in the case of $N = 128$, $m_\beta = 2$, $n = 4$, and by using look-up Table I, the total number of bits generated by OFDM block is 192 for JKG algorithm. The summary of the basic steps of IKG and JKG algorithms is presented in Fig. 4.3.

Due to channel decorrelation assumption, the generated key bits at legitimate and illegitimate nodes for IKG and JKG approaches will be different. The reason is that, even though the illegitimate node applies the same key generation method as the legitimate node, due to different channel responses compared to the legitimate node, the resultant key bits are different.

4.3 Simulation Results

In this section, simulation results are presented to demonstrate and analyze the effectiveness of the proposed algorithm. A practical SISO-OFDM system with $N = 128$ subcarriers and a CP of length L is considered. The total number of subblocks in each OFDM block is $N/n = 32$ with $n = 4$, and $m_\beta = 2$. Note that the values of N, G, n, and m_β have different effects on the proposed algorithm. However, the current simulations present one example of these cases. An identically independently distributed (i.i.d.) block-fading channel with coefficients having Rayleigh distribution is considered. The length of the multi-path channel between any communicating node pair is equal to $L = 9$ samples, where exponentially decaying power delay profile is considered [90].

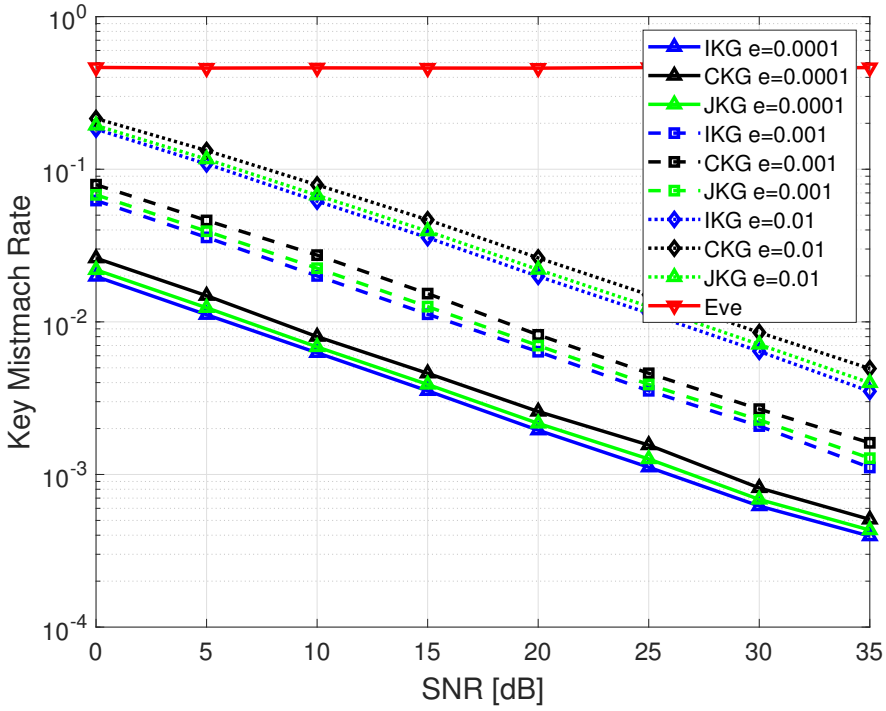


Fig. 4.4: KMR versus SNR performance under imperfect channel reciprocity and imperfect channel estimation for IKG, JKG, and CKG approaches.

The performance comparisons between IKG, JKG, and conventional key generation (CKG) approaches are presented here. IKG and JKG algorithms are explained earlier while the CKG approach is based on key generation from the amplitudes of estimated channel coefficients by comparing them with their mean [91]. The effectiveness of the proposed algorithm is presented in terms of KMR and KGR [92]. Moreover, the randomness of the key bits is evaluated by using a statistical test suite provided by NIST. Furthermore, the effects of imperfect channel reciprocity and imperfect channel estimation that exist due to noise, interference, and synchronization errors are taken into consideration [93]. The estimated channel along with the effect of imperfections at Alice and Bob can be given as: $\hat{\mathbf{H}}^{\mathbf{f}}_{\mathbf{ba}} = \mathbf{H}^{\mathbf{f}} + \mathbf{\Delta H}^{\mathbf{f}}_{\mathbf{ba}}$ and $\hat{\mathbf{H}}^{\mathbf{f}}_{\mathbf{ab}} = \mathbf{H}^{\mathbf{f}} + \mathbf{\Delta H}^{\mathbf{f}}_{\mathbf{ab}}$, respectively, where $\mathbf{H}^{\mathbf{f}}$ represents the perfect channel. $\mathbf{\Delta H}^{\mathbf{f}}_{\mathbf{ba}}$ and $\mathbf{\Delta H}^{\mathbf{f}}_{\mathbf{ab}}$ are modeled as independent complex Gaussian noise vectors with zero mean and error variance $\sigma^{\mathbf{2}}$, where $\sigma^{\mathbf{2}} = e \times 10^{\frac{-SNR_{dB}}{10}}$, wherein $e \in \mathbb{R}$ is a scale that corresponds to estimator quality. It should be noted that the quality of the estimator directly affects the error

variance value of the estimated channel such that better quality estimator results in lower values of error variance, σ^2. In the current work, three estimators with different qualities that correspond to three different values of e are considered such as $e \in \{0.01, 0.001, 0.0001\}$.

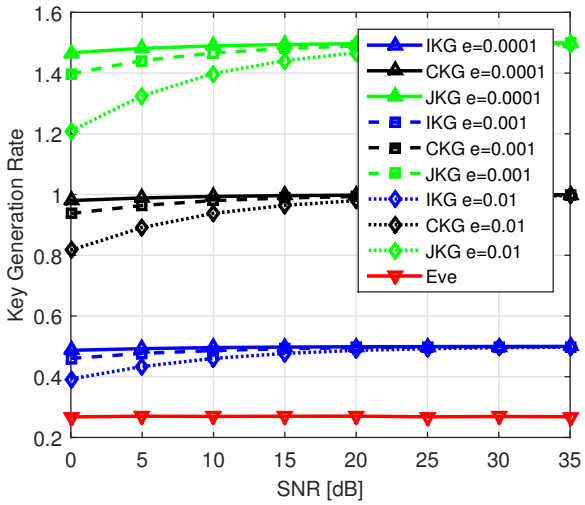


Fig. 4.5: KGR versus SNR performance under imperfect channel reciprocity and imperfect channel estimation for IKG, JKG, and CKG approaches.

Fig. 4.4 presents KMR versus signal to noise ratio (SNR) plots between the generated key at Alice and Bob under imperfect channel assumption for IKG, JKG, and CKG approaches, where imperfections are assumed to be independent at legitimate nodes but with equal error variance value. It is observed that as the values of σ^2 decreases by reducing the values of e from 0.01 to 0.0001, the KMR for all of the algorithms decreases. It is also observed that the key generation for the IKG approach is better than the JKG approach while the KMR for the CKG approach is worst compared to others. Moreover, Fig. 4.4 also presents the KMR at the eavesdropper that generates key bits based on its channel by using the JKG approach. Thanks to channel decorrelation, there is a significant gap between the KMR at the legitimate node and Eve as compared to all the cases at legitimate nodes.

Fig. 4.5 presents the KGR (efficiency= bits/channel coefficient) versus SNR comparisons between IKG, JKG, and CKG approaches. It is observed from the

figure that as the values of e decrease, from 0.01 to 0.0001, the KGR improves for all approaches. It is also observed that the JKG approach outperforms both the CKG and IKG approaches in terms of KGR while the KGR of CKG approach is in between KGR of JKG and IKG approaches as shown in Fig. 4.5. Moreover, considering the KMR and KGR of CKG and JKG approaches from Fig. 4.4 and Fig. 4.5 jointly, it is observed that due to the exploitation of the proposed dimension, there is an increase in the overall key rate in the JKG approach compared to the CKG approach without degrading the KMR performance. More specifically, there is a 50 % increase in key rate as presented by the JKG plot compared to the CKG approach due to the involvement of the proposed dimensions of key generation. Moreover, Fig. 4.5 also presents the KGR performance of Eve, where it is using the JKG approach based on its channel. It is observed that Eve has the worst performance in terms of KGR compared to all the cases with respect to generated key bits at the legitimate nodes due to channel decorrelation.

In order to evaluate the randomness of the key bits a statistical test suite provided by NIST is used [94]. There are 15 tests in NIST's statistical test suite, where each test evaluates a particular random characteristic. For example, the periodic features of the sequence are detected by the DFT test, the proportion of ones and zeros are detected by the frequency test. All of these tests return a $P-value$ in order to check the randomness of the sequence. The $P-value$ is compared with a significance value, α, where range of α is $[0.001, 0.01]$. The sequence is accepted as random if $P-value > \alpha$, otherwise it is considered as non-random, where we choose $\alpha = 0.01$ [95]. The generated bitstream by our algorithm meets the input size recommendation of 8 NIST tests because the remaining tests require a very long sequence e.g 10^6. Therefore, we ran 8 tests, which still satisfies the requirements of NIST [95] [94]. It is observed from Table II that the generated bitstream by the proposed algorithms (IKG and JKG) passed the conducted randomness tests of the NIST test suite. More specifically, the $P-values$ for our case are greater than 0.01.

Table 4.2: NIST statistical test suite results. The $P-value$ from each test is listed below. To pass a test, the $P-value$ for that test must be greater than 0.01.

	$P-values$ **(IKG)**	$P-values$ **(JGK)**
Frequency	**0.774**	**0.762**
Block frequency	**0.820**	**0.796**
Runs	**0.748**	**0.723**
Longest run of 1s	**0.601**	**0.531**
DFT	**0.782**	**0.741**
Serial	**0.611** **0.590**	**0.583** **0.501**
Approx. Entropy	**0.514**	**0.482**
Cumulatic sum (forward)	**0.672**	**0.625**
Commulative sum (reverse)	**0.601**	**0.599**

4.4 Conclusion and Future Directions

In this work, efficient algorithms are proposed for secret key generation from the wireless channel, where key bits are not only generated by amplitudes of the subcarriers but also by the indices of subcarriers corresponding to highest channel gains. Specifically, in the first step, the communicating nodes convert the correlated frequency response of the channel at them into random order by exploiting random interleaver. Afterwards, the estimated channel response in the frequency domain at them is partitioned into small subblocks. Finally, the key bits are generated by both amplitudes of individual subcarriers by comparing with their mean as well as by indices/positions of good sub-channels in each subblock by employing a look-up table. The proposed novel dimensions for secret key generation results in the enhancement of overall KGR without degrading overall performance as shown by simulation results. More specifically, there is a 50 % increase in key rate as shown by JKG performance compared to the CKG approach due to the involvement of the proposed dimensions of key generation. For future work, different variations of the proposed algorithm assuming different activation ratios and block sizes can be considered. In addition, the proposed

algorithm of secret key generation can be extended to other domains such as time, space, and code domains.

Chapter 5

Enhancing Physical Layer Security of OFDM Systems Using Channel Shortening

5.1 Introduction

Due to the broadcast characteristics of wireless communication services, it is inherently vulnerable to eavesdropping and spying. Thus, designing effective and efficient security techniques is one of the most crucial requirements [92]. The conventional security techniques are mainly focused on cryptography, but they are not sufficient due to their high complexity in key's establishment and management, especially for future decentralized network [93]. Nowadays, physical layer security (PLS) techniques have drawn a lot of attention due to their ability to solve the challenges in the conventional encryption-based techniques. The PLS techniques provide security by means of exploiting the impairments of the wireless channel, such as noise, fading and interference, etc.

Among the many emerging PLS fields, securing OFDM transmission has become one of the most important areas of PLS research [93]. This is due to the

fact that OFDM is the most popularly used technique in current and for future wireless systems because of its high spectral efficiency, and ability to combat frequency-selective fading channels [93]. In the literature, a lot of PLS techniques have been proposed to secure OFDM. These techniques include: a) secret key generation [96], b) artificial noise (AN) [97], c) signal feature suppression [98], and d) channel based adaptive transmission, such as adaptive power allocation and pre-equalization based on Bob's channel for PLS [50].

In OFDM, to combat multipath fading effects of the channel, a cyclic prefix (CP) is inserted between OFDM blocks [99]. The CP ensures immunity to multipath effect only if the length of the channel delay spread is less than or equal to the CP. Otherwise, it will destroy the orthogonality of subcarriers and will cause ISI. However, the length of channel delay spread is very long for certain outdoor multipath channels. Thus, they require longer CP, causing more spectral and power efficiency loss [100].

To avoid this efficiency loss due to longer CP, one solution is to reduce the length of effective channel by means of channel shortening (CS) [99]. In the literature, a lot of techniques have been proposed in order to design coefficients of the channel shortening filter by using time or frequency domain characteristics of the channel. The proposed methods in [99] [100] [101] tried to shorten the channel on the basis of its time domain characteristic. These techniques try to maximize the energy inside the window that contains $V + 1$ consecutive samples of the channel, where V is CP length. In [102], a method of CS is proposed, in which the channel is shortened by removing the zeros of an all-zero wireless system model with the help of series of cascaded feedback filters. The proposed techniques in [103] [104] [105] exploit frequency domain characteristics of channel to design filter coefficients. These techniques try to maximize sub-channel Signal to Interference and Noise Ratio (SSINR) to enhance the data rate. The above mentioned techniques require training sequence for CS operation and in order to avoid transmission of training sequence, blind CS base schemes have been proposed [106].

In the literature, CS techniques are mainly applied at receiver side, and only

a few studies reported its use at the transmitter. To the best of the authors' knowledge, no work has been reported to use CS technique for PLS. Therefore, in this study, a simple approach to provide PLS by using CS is presented. More specifically, the basic idea is to use smaller CP, and apply CS method at transmitter side, and design the equalizer coefficients in such a way that the effective channel for Bob does not cause ISI, while effective channel for Eve causes ISI. Although CS at the transmitter looks similar to pre-equalization but they are different, because in CS the channel is shortened in time domain, while in pre-equalization, the amplitude and phase of the channel are equalized in frequency domain [99], [100]. Thus, CS has lower peak to average power (PAPR) and is more robust to channel estimation errors as compared to pre-equalization [99]. It is shown by simulation results that the use of smaller CP and CS schemes with respect to Bob's channel at transmitter can provide QoS based security.

The rest of the paper is organized as follows: The system model is presented in Section II, followed by the proposed approach for using CS for security in Section III. Section IV presents simulation results, and the paper is concluded in Section V.

5.2 System Model and Preliminaries

Our system model consists of a legitimate transmitter (Tx), called Alice, that wants to have a secure communication with a legitimate receiver (Rx), called Bob, in the presence of a passive eavesdropper, called Eve, as presented in Fig. 5.1. The notations $h_b(h_{ab})$ and $h_e(h_{ae})$ denote slow varying rayleigh fading coefficients from source to destination and source to Eve, respectively, while n_{bk} and n_{ek} represent additive white Gaussian noise (AWGN) at source to destination and source to Eve, respectively. Channel reciprocity property is also adopted, where the channel from Alice to Bob can be estimated from the channel of Bob to Alice in TDD system, i.e. $h_{ab} = h_{ba}$.

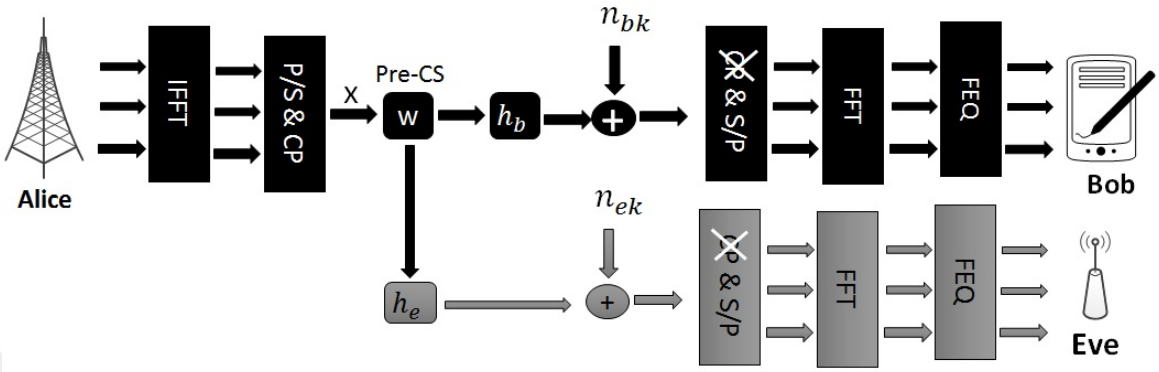


Fig. 5.1: System Model.

5.3 Proposed Approach to Use CS for Security

Consider a simplied OFDM based model with CS shortener $w(n)$ as presented in Fig. 5.1. At the Tx, the total number of modulated symbols in one block is N, that also represents the utilized frequency spectrum. Thus, the frequency domain of each OFDM symbol can be represented as $X = [X_0 \ X_1 \ ..... \ X_{N-1}] \in C^{[N\times 1]}$. These blocks are then passed through an IFFT process, which maps the frequency domain data symbols to time domain points represented by $x = [x_0 \ x_1 \ ... \ x_{N-1}] \in C^{[N\times 1]}$. To avoid ISI, a CP of length V is inserted at the beginning of the block. The resultant signal is then passed through time domain channel shortener, $w(n)$, as presented in Fig. 5.1. Finally, the signal is transmitted through the channel, and reaches to both Bob and Eve. The output of linear time-invariant wireless OFDM with respect to Bob's channel without $w(n)$ is given by

$$y_b(n) = h_b(n) * x(n) = \sum_{k=0}^{L-1} h_b(k)x(n-k). \tag{5.1}$$

We can re-write the above equation as follows

$$y_b(n) = h_{b0}x(n) + \sum_{k=1}^{v} h_b(k)x(n-k) + \sum_{k=v+1}^{L-1} h_b(k)x(n-k). \tag{5.2}$$

The output of linear time-invariant wireless OFDM with respect to Eve's channel without $w(n)$ is given by

$$y_e(n) = h_e(n) * x(n) = \sum_{k=0}^{L-1} h_e(k)x(n-k) \tag{5.3}$$

The above equation can be reformulated as

$$y_e(n) = h_{e0}x(n) + \sum_{k=1}^{v} h_e(k)x(n-k) + \sum_{k=v+1}^{L-1} h_e(k)x(n-k). \tag{5.4}$$

The first term at the right side of equation 2 and 4 is the desired term for Bob and Eve, respectively, while the second and third terms are the undesired ones. The second term can be handled by CP, while the third term causes ISI. More specifically, if the channel length is equal to or less than CP then CP can remove ISI completely but if the channel length is greater than CP then it can destroy the orthogonality of the system, and causes performance degradation. This is the basic principle that is used for CS based security concept.

To avoid efficiency loss due to longer CP, smaller CP is preferred with channel shortening techniques. In the literature, majority work is based on channel shortening techniques at receiver side and no work has been reported related to PLS based CS. Therefore, in this work, CS techniques are applied in such a way that they not only provide spectral and power efficiency, but also provide QoS based security. Our idea can be applied by using two approaches:

(A) Approach 1: Shortening based on Bob's and Eve's channels.

(B) Approach 2: Shortening based on Bob's channel only.

5.3.1 Approach 1: Shortening based on Bob's and Eve's Channels

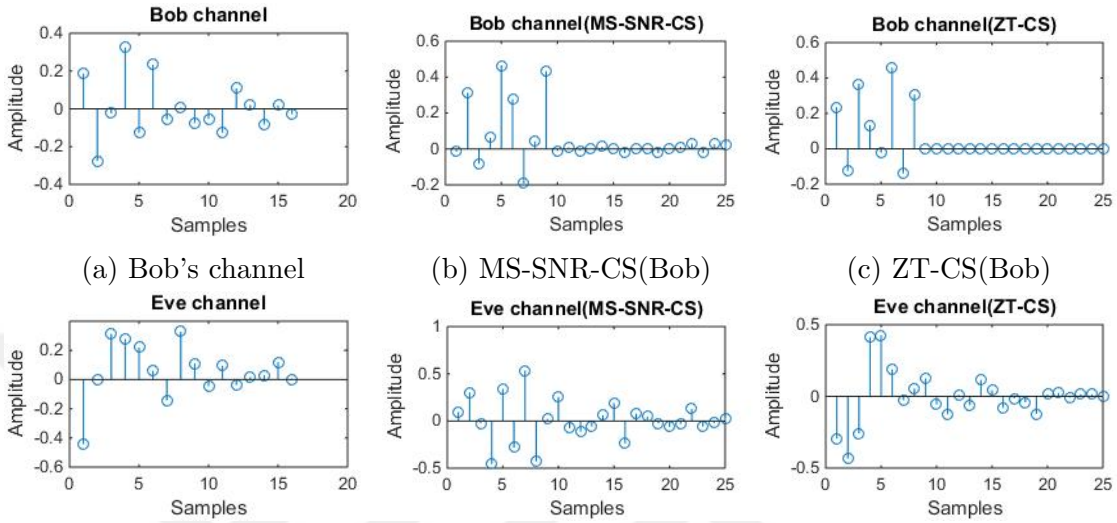
We use smaller CP and apply CS technique at the transmitter by designing $w(n)$ with respect to channel of both Bob and Eve, simultaneously. More specifically, the filter coefficients $w(n)$ are designed in such a way that the energy of the effective channel at Bob, $h_{effb} = w(n) * h_b(n)$, gets concentrated in a window of $V + 1$ consecutive samples of effective channel, while the energy of effective channel at Eve, $h_{effe} = w_b(n) * h_e(n)$, gets concentrated out of window of length $(V + 1)$. In this way, CP is enough for Bob, while CP is not enough for Eve, so ISI is caused at Eve.

5.3.2 Approach 2: Shortening based on Bob's Channel only

We use smaller CP and apply CS technique at the transmitter by designing $w(n)$ with respect to the channel of Bob only. In this approach, $w(n)$ are designed in such a way that the energy of the effective channel at $h_{effB} = w(n) * h_b(n)$ gets concentrated in the window of length $V + 1$ while the energy of tails around it get minimized out of window.

Both of the above mentioned approaches can provide QoS based security. It should be noted that the first approach can provide more security, but it requires channel state information of Eve which is not always available. Thus, in this work, we focus on the second approach. To show the effectiveness of second approach, we design CS coefficients by using two channel shortening techniques based on Bob's channel and we apply them at the transmitter side. As the coefficients are designed with respect to Bob's channel, this approach not only provides spectral and power efficiency but also QoS based security. These techniques are as follows:

1. Maximum shortening SNR (MS-SNR)-based CS.



(a) Bob's channel (b) MS-SNR-CS(Bob) (c) ZT-CS(Bob)

(d) Eve's channel (e) MS-SNR-CS(Eve) (f) ZT-CS(Eve)

Fig. 5.2: Channel at Bob and Eve with MSSNR-CS and ZT-CS.

2. Z-Transform (ZT)-based CS.

5.3.2.1 Maximum Shortening SNR (MS-SNR)-based CS

The MS-SNR-based technique [99] helps to design equalizer coefficients such that the maximum energy lies just in a portion of the effective channel that is less than or equal to $V+1$. Let us suppose H_b is the toeplitz matrix for h_b and $h_{effb} = H_b w$ is the effective channel after passing through equalizer. Let us suppose $p_{winb} = H_{winb} w$, represents a window of $V+1$ consecutive samples of h_{effb} where we want to concentrate maximum energy and $p_{wallb} = H_{wallb} w$ represents the remaining $L + t - V - 2$ samples, where L is the length of channel, t is length of effective channel, V is CP length and H_{winb} & H_{wallb} are parts of H_b corresponding to p_{winb} and p_{wallb}, respectively.

We can define MS-SNR problem as to "maximize $||p_{winb}||$ subject to the constraint $||p_{wallb}|| = 1$" . The problem can be defined as

$$\max_{w}(w^T B w) \quad subject\ to \quad w^T A w = 1, \tag{5.5}$$

$$A = H_{wallb}^{T} H_{wallb}, \quad B = H_{winb}^{T} H_{winb}. \tag{5.6}$$

The solution of the above equation leads to the equalizer coefficients $w(n)$ that satisfy the generalized eigenvector problem given as

$$Bw = \lambda Aw. \tag{5.7}$$

The solution of the above problem for $w(n)$ will be the generalized eigenvector corresponding to the largest generalized eigenvalue λ. Alternatively, we can also define MS-SNR problem as to "minimize $||p_{wallb}||$ subject to the constraint $||p_{winb}|| = 1$". The solution for $w(n)$ will be the generalized eigenvector corresponding to the smallest generalized eigenvalue $\bar{\lambda}$.

5.3.2.2 Z-Transform (ZT)-based CS

The impulse response of wireless channel can be represented as a finite impulse response (FIR) filter thus it has only zeros. In this method the channel is shortened by removing zeros of wireless channel with the help of series of cascaded feedback filters. In order to derive filter coefficients based on Bob's channel, we apply Z-transform on both sides of equation (1) and then simplify it by using partial fraction as follows

$$H_b(z) = \frac{Y_z}{X_z} = h_0 \prod_{k=0}^{L-2} (1 - r_k z^{-1}). \tag{5.8}$$

where r_k is the root (also know as the zero) of H(z). The inverse of the factor "$(1-r_k z^{-1})$" is stable and causal if the zero "r_k" is inside unit circle, which ensures that the system $a_k(z) = 1/(1-r_k z^{-1})$ and $H_b(z)a_k(z)$ are both causal and stable. Thus, the zeros of channel can be canceled by using $a_k(z) = 1/(1 - r_k z^{-1})$, that can be implemented by using feedback with lower complexity, such that one zero of channel can be canceled by one feedback filter. In order to cancel e taps of channel, we require e feedback filter. Thus, CS based shortener $w(n)$ consists of series of cascaded feedback filters $a_k(z)$.

From the above mentioned techniques, the coefficients for CS based techniques are calculated based on Bob's channel and applied at the transmitter. Finally, signal passes through h_b and h_e and reaches to Bob and Eve. After receiving, each of them will first discard the CP and then perform FFT process. After that, both receivers will apply frequency domain equalization. The effective channel at Bob, $h_{effb(n)} = h_b(n) * w(n)$, does not cause ISI because CP is enough to combat ISI. The received signal at Bob with $w(n)$ is given by

$$y_b = \sum_{k=1}^{L-1} h_{effB}(k)x(n-k). \tag{5.9}$$

The effective channel at Eve, $h_{effe(n)} = h_e(n) * w(n)$, causes ISI because CP is not enough at Eve. The received signal at Eve with $w(n)$ is given by

$$y_e = \sum_{k=1}^{L-1} h_{effE}(k)x(n-k) \tag{5.10}$$

Due to ISI there will be a degradation for Eve's BER performance that will provide QoS based security.

5.4 Simulation Result

In this section, the channel impulse response (CIR) at Bob and Eve before and after CS techniques as well as the simulation results using bit error rate (BER) as a metric [96], [107] are presented to analyze the effectiveness of the proposed method. The basic simulation parameters are presented in Table 5.1.

In Fig. 5.2 CIR at Bob and Eve before and after the channel shortening techniques is presented. Fig. 5.2. a, 5.2. b and 5.2. c present the CIR at Bob before shortening, Bob with MS-SNR-based CS and Bob with ZT-based CS, respectively. It should be noted that MS-SNR-based CS algorithm concentrates maximum energy of effective channel in window of $V + 1$ length as much as possible, and minimizes energy out of window as much as possible, but there is still some leakage outside the window that causes some ISI. On the other hand,

Table 5.1: System parameters

Modulation	QAM
Channel	Rayleigh fading channel
Bob's Channel length h_b	16
Eve's Channel length h_e	16
FFT size	64
CP length (required)	16
CP length (used)	8

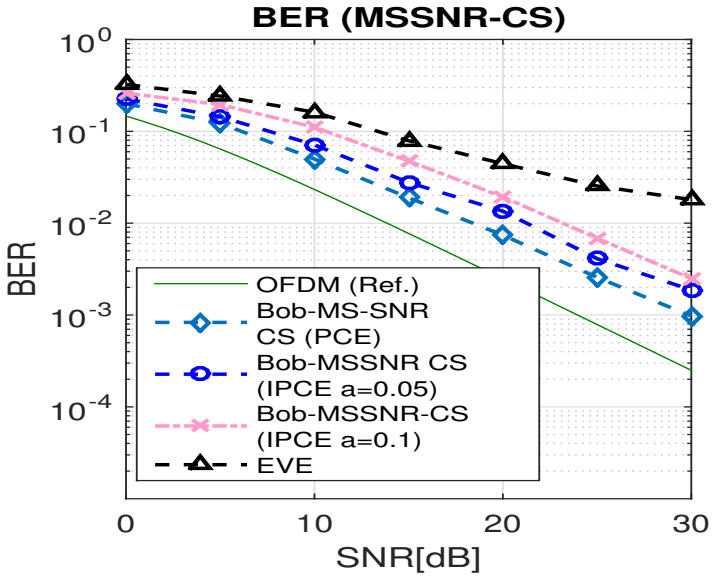


Fig. 5.3: BER performance for MS-SNR-CS.

ZT-based algorithm can eliminate ISI completely as compared to MS-SNR and there is negligible leakage.

On the other hand, Fig. 5.2. d, 5.2. e and 5.2. f show the CIR at Eve before shortening, Eve with MS-SNR-based CS and Eve with ZT-based CS, respectively. It is observed that MS-SNR and ZT-based CS algorithm do not help too much to Eve to concentrate energy inside window of $V+1$ because $w(n)$ is designed based on Bob's channel which is different from Eve's channel due to spatial decorrelation nature of the wireless channel. Thus, Eve will suffer from the leakage in window out of $V+1$ and CP will not be enough for Eve.

In Fig. 5.3 and Fig. 5.4, simulation results are shown by using BER as a metric. In all simulations, the effect of imperfect channel estimation that may occur due to possible noise, interference etc. is taken into account.

The imperfectly estimated channel at Alice and Bob can be modeled by adding intentional errors ($\Delta h_{T/R}$) to the perfect channel (h_b) at both the transmitter and receiver and is given by $\hat{h}_{T/R} = h_b + \Delta h_{T/R}$, where Δh is modeled as an independent complex Gaussian noise vectors with zero mean and error variance $\sigma^2 = a \times 10^{\frac{-SNR_{dB}}{10}}$, where a represents different estimation qualities [107], [108].

In Fig. 5.3 and Fig. 5.4 the BER performance at Bob and Eve for MS-SNR and ZT-based CS algorithm is presented. The results show BER performance at Bob under different estimation qualities with a=0 (perfect estimation), a=0.05 and a=0.1. It is shown in both cases that there is some degradation due to imperfect channel estimation. However, this degradation can be overcome by using training sequence of longer length and by using higher power. Furthermore, Fig. 5.3 and Fig. 5.4 also present performance of conventional OFDM (OFDM-Ref.) for comparison. In OFDM-Ref. no CS is applied and longer CP corresponding to channel length (L) is used. It is shown that the performance of ZT-based CS is approximately same as OFDM-Ref., while there is a small degradation in the performance of MS-SNR based CS as compared to both ZT-based and OFDM-Ref. The reason is that although MS-SNR-based CS algorithm concentrate the energy of effective channel in window of $V + 1$ as much as possible but there is still some leakage as presented in Fig. 5.2. b.

Moreover, Fig. 5.3 and Fig. 5.4 also present performance for Eve. It is observed that there is a BER performance degradation at Eve for both MS-SNR and ZT based CS. The reason is that the equalizer coefficients $w(n)$ are designed based on Bob channel and $w(n)$ will not help Eve to shorten its channel and thus the effective channel causes ISI and detroies the orthogonality at Eve. The BER performance at Eve is greater than 10^{-2}, which can provide QoS based security [107]. More specifically, it can secure voice communication between legitimate parties as per LTE [107]. Hence, our algorithm can provide QoS based security.

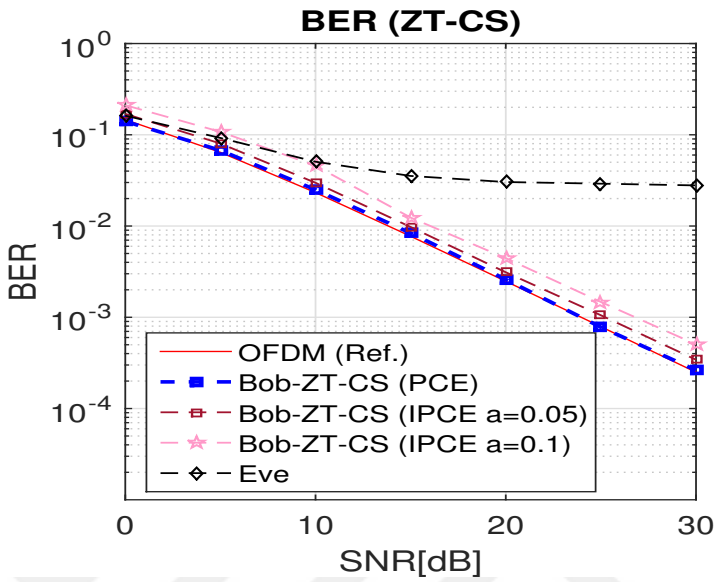


Fig. 5.4: BER performance for ZT-CS.

5.5 Conclusion

In this work, a practical spectral and power efficient security method is presented that is based on channel shortening. Channel shortening equalizer coefficients are designed based on Bob's channel and CS is used at transmitter in such a way that the effective channel ensures no ISI at Bob, while causing ISI and performance degradation at Eve, thus, QoS based security can be provided. The simulation results are given for both perfect and imperfect channel estimation to demonstrate the effectiveness and robustness of the proposed algorithm. The proposed scheme can provide QoS based security and can successfully secure voice communication between legitimate parties. The idea can be extended to provide security to any single carrier or multi carrier CP based system.

Chapter 6

Adaptive OFDM–IM for Enhancing Physical Layer Security and Spectral Efficiency

6.1 Introduction

The inherent broadcast characteristic of wireless communication makes it vulnerable to the passive eavesdropping. Conventionally, security techniques in the upper layers, such as cryptography based techniques, have been employed for secure transmission. However, such security techniques may not be adequate for future decentralized networks due to their high complexity in implementation and computation [109]. Furthermore, the emergence of powerful computing devices makes these techniques vulnerable to sophisticated adversaries. In order to cope up with these problems, Physical Layer Security (PLS) techniques have attracted a lot of attentions [110]. PLS techniques exploit the dynamic features of wireless communications, such as channel randomness, interference and noise, etc., to prevent the eavesdropper from decoding data while ensuring that the legitimate user can decode it successfully [109]. In the literature, practical signal processing based PLS techniques are proposed in order to secure communication between

legitimate parties [111], [112].

On the other hand, Index Modulation (IM) is an emerging technique for future wireless networks because of its higher Energy Efficiency (EE) and controllable Spectral Efficiency (SE) [113]. Spatial Modulation (SM) and OFDM-IM are two well known applications. Especially, OFDM-IM has been studied intensively in the literature [113], [114]. Unlike conventional OFDM, which sends data via M-ary signal constellation, in OFDM-IM, data is sent by both M-ary signal constellation and indices of the subcarriers. Due to high EE and adjustable SE, it is considered not only for Machine Type Communication (MTC) but also for high speed wireless communication systems [113], [115]. There are a lot of interesting works for enhancing spectral efficiency of SM and OFDM-IM. In [116], pre-coding based technique is proposed in which spatial modulation works in both the in-phase and quadrature parts of the received signals, thus conveying additional information bits compared with conventional generalized precoding-aided spatial modulation. In [117], information is conveyed through multiple distinguishable modes and their full permutations. Authors proposed frequency index modulation technique and a joint code-frequency index modulation techniques for enhancing energy and spectral efficiency in [118] and [119], respectively. The proposed techniques are simple and can reduce PAPR without sacrificing data rate. In [120], authors proposed a scheme to enhance the spectral and energy efficiency by using initial conditions to generate different chaotic sequences that can convey extra bits per transmission.

In the following, we will first explain some of the related and popular PLS techniques for OFDM and then for SM and finally for OFDM-IM. In the literature, many promising PLS techniques have been proposed for OFDM. In [121], secret key generation based techniques are proposed for OFDM system. The basic idea is to extract random sequence from the wireless channel. Motivated by the effectiveness of Artificial Noise (AN) for providing PLS, authors in [122] added AN signal on top of OFDM data signal in such a way that when the AN passes through the channel it gets accumulated in Cyclic Prefix (CP) at the legitimate receiver only. Thus, it causes no interference at the legitimate receiver, but degrades the performance of Eve. In [123], signal feature suppression based PLS technique

was proposed. In this technique certain signal features are suppressed to avoid eavesdropping, such as CP periodicity feature concealing. Furthermore, adaptation based security techniques are also very popular PLS techniques in which transmitter parameters are adjusted in order to fulfill the Quality of Service (QoS) requirement of the legitimate receiver only, for example, adaptive modulation and coding with Automatic Repeat Request (ARQ) [124], fading based sub carrier activation technique [125], optimal power allocation based techniques [126], channel shortening [127], OFDM-subcarrier index selection for enhancing PLS [128], etc. It may be noted that adaptation based techniques, such as adaptive modulation and coding can jointly enhance the security and spectral efficiency of wireless systems [126].

Now moving from PLS techniques for OFDM to PLS for IM. There are a few interesting PLS techniques proposed in the literature for SM in MIMO systems [129]- [130]. In [129], authors proposed transmit precoding based PLS techniques for SM. Moreover, jamming signal based PLS techniques are presented in [131]. In [132], authors proposed PLS techniques based on exploiting the channel reciprocity of Time Division Duplex (TDD) system to redefine the transmit antenna indices. However, the proposed technique cannot secure data symbol modulation. In order to solve this deficiency, the authors in [133] proposed a technique in which the rotation of both the indices of transmit antennas and constellation symbols based on the channel state information of the legitimate receiver are exploited. Thus, securing both index modulation and data symbol modulation. To the best of authors' knowledge, the first work related to PLS in OFDM-IM has recently been introduced in [130]. The authors investigate the randomized mapping rules based on channel reciprocity in TDD mode in order to secure both data symbol modulation and index modulation but in that work spectral efficiency is not taken into account.

In the literature, majority of the works related to PLS are focused on the enhancement of security, but only a few works are reported to focus on the joint consideration of both spectral efficiency and security. Moreover, there are some techniques in which security is achieved at the cost of loss in resources.

Inspired by the need for joint consideration of security and SE, in this paper, we propose algorithms for the enhancement of PLS of OFDM-IM and for the quality of service (QoS) based communication in order to enhance SE of OFDM-IM. The proposed algorithms are based on adaptive subcarrier switching and adaptive modulation. More specifically, three approaches are proposed, namely OFDM with Adaptive Index Modulation and Fixed Constellation Modulation (OFDM-AIM-FCM) for enhancing PLS and SE, OFDM with Adaptive Index Modulation and Adaptive Constellation Modulation (OFDM-AIM-ACM) for enhancing PLS and SE and OFDM with Variable Index Modulation and Variable Constellation Modulation (OFDM-VIM-VCM) for QoS based communication in order to enhance SE. In particular, the first two approaches are based on channel based adaptation of subcarrier activation ratios and constellation modulation orders of subblocks in OFDM-IM by utilizing channel reciprocity concept in TDD mode while the third approach is based on QoS based adaptation. The works in [116] and [117] focus on spectral efficiency alone without considering security concerns while first two proposed schemes provide security with some enhancement in spectral efficiency. The scheme in [117] and our third proposed algorithm both target enhanced SE, while the proposed technique keeps the benefits of OFDM-IM, namely low ICI and high EE, [117] does not keep these benefits.

Notation: Bold, lowercase and capital letters are used for column vectors and matrices, respectively. rank ($\mathbf{A}$) and det ($\mathbf{A}$) denote the rank and determinant of $\mathbf{A}$, respectively. $\lambda_i(A)$ is the i_{th} eigenvalue of $\mathbf{A}$. The expectation of an event is denoted by $E\{.\}$ and $P(.)$ stands for probability of an event. $\mathcal{S}$ denotes the complex signal constellation of size M. $\lfloor . \rfloor$ is the floor function and $Q(.)$ denotes the tail probability of the standard Gaussian distribution. $\mathcal{CN}(0, \sigma_X^2)$ represents the distribution of a circularly symmetric complex Gaussian random variable X with variance σ_X^2. $(.)^H$ and $(.)^T$ denote Hermitian transposition and transposition, respectively.

6.2 System Model and Preliminaries

In this work, we consider a Single Input Single Output (SISO) OFDM-IM system. The basic system model consists of a legitimate Transmitter (Tx), Alice, that wants to communicate securely with a legitimate Receiver (Rx), Bob, in the presence of an illegitimate node, Eve, as shown in Fig. 6.1, where TDD is considered as an operational mode. The notations $\mathbf{h}_{ab}(\mathbf{h}_b) \in^{[1\times L]}$ and $\mathbf{h}_{ae}(\mathbf{h}_e) \in^{[1\times L]}$ denote the slow varying multi-path Rayleigh fading exponentially decaying channel from Alice to Bob and Alice to Eve, respectively, where L is the length of the channel. In this work, Eve is considered to be passive, and hence there is no knowledge of Eve's channel at Alice. Moreover, it is also assumed that Eve is not very close to Bob such that Bob and Eve will have independent channel realizations [128]. In addition, the property of channel reciprocity is also adopted in this work, where the channel from Alice to Bob ($\mathbf{h}_{ab}$) can be estimated from the channel of Bob to Alice ($\mathbf{h}_{ba}$) in TDD.

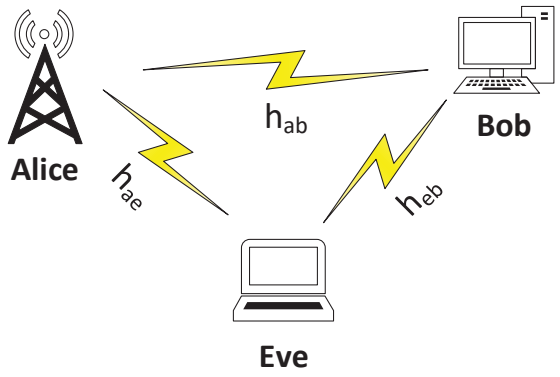


Fig. 6.1: System Model.

6.3 Adaptive OFDM-IM Model and Proposed Algorithms

In this Section, basic concepts related to OFDM-IM with respect to adaptivity as well as proposed algorithms for enhancing PLS and SE are presented.

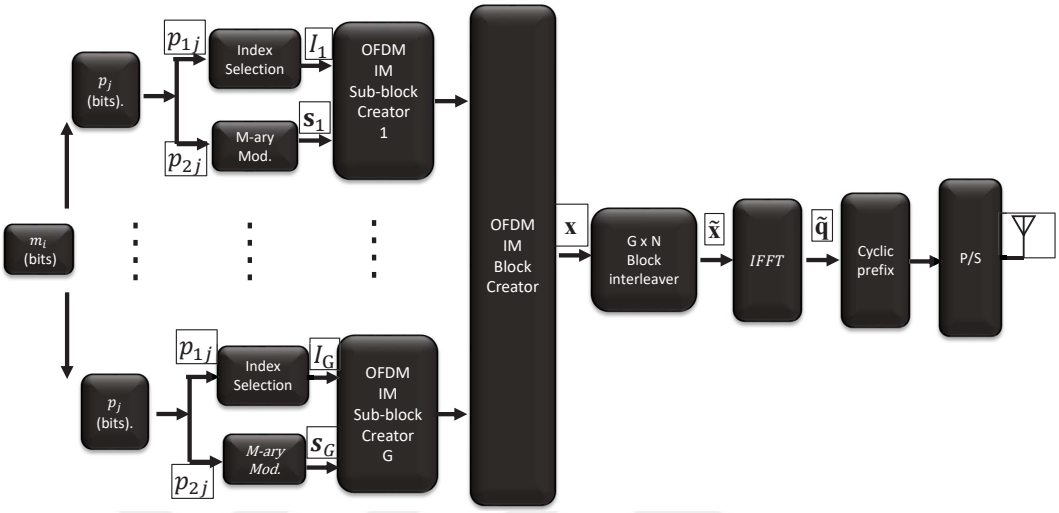


Fig. 6.2: Basic OFDM-IM Tx.

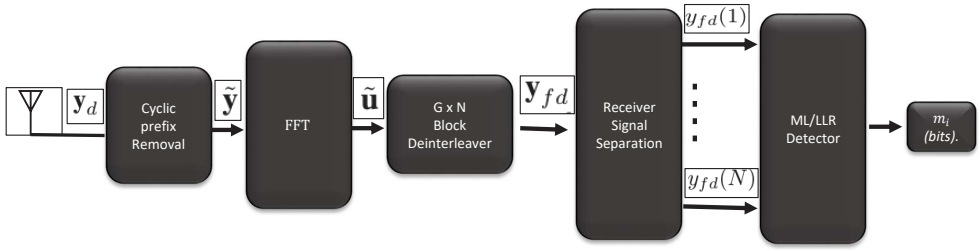


Fig. 6.3: Basic OFDM-IM Rx.

6.3.1 Adaptive OFDM-IM Model

In this subsection, OFDM-IM model [113], [114] with respect to Channel Based Adaptation (CBA) is explained. In this system, we employ a simplified OFDM-IM model as presented in Fig. 6.2 and Fig. 6.3, where Fig. 6.2 presents the OFDM-IM transmitter (Tx) while Fig. 6.3 presents the OFDM-IM receiver (Rx), respectively. Let us suppose that m_i number of information bits, corresponding to i_{th} block, enters the OFDM-IM for the transmission, where the value of m_i is different for different OFDM-IM blocks due to CBA and will be explained in subsection III.B. These m_i bits are split into G groups, such that each group contains p_j bits, where $j \in \{1, ..., G\}$. The p_j may be different for different groups based on CBA. The total number of bits in i_{th} block can be represented

as follows:

$$m_i = \sum_{j=1}^{G} p_j \tag{6.1}$$

In OFDM-IM, the subcarriers are also divided into G subblocks. The number of subcarriers in any subblock, β, is n, where $n = N/G$ and N is the total number of subcarriers in any OFDM-IM block. After that, p_j bits of each group are mapped to corresponding subblock, β. This mapping is done by means of symbols and by the indices of subcarriers based on CBA.

The p_j bits of each group are divided into p_{1j} and p_{2j} bits, where p_{1j} bits are carried by indices and p_{2j} bits are carried by symbols. More specifically, in each OFDM subblock, k_j out of n subcarriers are active and selected by index selector based on p_{1j} bits while the symbols corresponding to inactive subcarriers are set to zero. In the proposed work, each subblock may have different Subcarrier Activation Ratio (SAR), k_j/n, and Constellation Modulation (CM) order based on CBA. In this work, we consider four cases for SAR that are 1/4, 2/4, 3/4 and 4/4 and four cases of CM that are 2, 4, 8 and 16. The index selector of OFDM-IM uses a predefined look-up table for each subblock based on its SAR. Fig. 6.4 presents look up tables for SARs of 1/4, 2/4 and 3/4, while the case of SAR value of 4/4 does not require any lookup table because no information is sent by indices (Classical OFDM). The remaining p_{2j} bits are mapped on to M-ary data symbols, based on subblock CM, that modulates the active subcarriers. In this way, the information is conveyed by both indices of subcarriers and M-ary symbols that modulate the active subcarriers.

The selected indices are given by $I_\beta = \{i_{\beta,1}, ..., i_{\beta,k_j}\}$, where $\beta \in \{1, ..., G\}$, $i_{\beta,\gamma} \in \{1, ..., n\}$, and $\gamma \in \{1, ..., k_j\}$. Therefore, the total number of bits carried by the indices of all G groups in the i_{th} block is given by

$$m_{1i} = \sum_{j=1}^{G} p_{1j}, \tag{6.2}$$

$$p_{1j} = \lfloor \log_2 \binom{n}{k_j} \rfloor. \tag{6.3}$$

Hence, I_β has $c = 2^{p_{1j}}$ possible realizations. On the other hand, the total number of information bits carried by M-ary signal constellations are given by:

$$m_{2i} = \sum_{j=1}^{G} p_{2j}, \tag{6.4}$$

$$p_{2j} = k_j \log_2 M_j, \tag{6.5}$$

where M_j is the modulation order and k_j is the number of active subcarriers in each subblock. In this scheme, the total number of active subcarriers in each OFDM block is given as $K = \sum_{j=1}^{G} k_j$. The output of M-ary modulator is given as

$$\mathbf{s}_\beta = [s_\beta(1), \ldots, s_\beta(k_j)], \tag{6.6}$$

where $s_\beta(\gamma) \in \mathcal{S}$. It should also be noted that the signal constellation is normalized to have unit average power. Finally, the OFDM block creator uses I_β and $\mathbf{s}_\beta$ to create all of subblocks and then forms $N \times 1$ main OFDM-IM block by concatenation of G subblocks and is given by:

$$\mathbf{x} = [x_1, x_2, ..., x_N]^T. \tag{6.7}$$

where $x(\alpha) \in \{0, \mathcal{S}\}$, $\alpha \in \{1, ..., N\}$. After this point, the block $\mathbf{x}$ is passed through $G \times N$ interleaver to ensure that the subcarriers in each subblocks are affected by uncorrelated wireless fading channels.

The resultant OFDM block after interleaver, $\tilde{\mathbf{x}}$, is then passed through IFFT process, $\frac{N}{\sqrt{K}} IFFT\{\tilde{\mathbf{x}}\}$, which maps the frequency domain data symbols to time domain points represented as follows:

$$\tilde{\mathbf{q}} = [q_1, q_2, ..., q_N]^T \tag{6.8}$$

In order to avoid ISI, a CP of length (L_{cp}) is added at the beginning of each block, where L_{cp} is assumed to be equal to or greater than the channel delay spread. Finally, the resultant signal $\tilde{\mathbf{q}} \in C^{[N+L\times 1]}$ is transmitted through the Rayleigh fading channel, which is assumed to be constant during the transmission of each OFDM block, and reaches to both Bob and Eve. The baseband signal received at Bob can be represented as

$$\mathbf{y}_b = \mathbf{h}_b * \tilde{\mathbf{q}} + \mathbf{z}_b, \tag{6.9}$$

where $\mathbf{h}_b$ is the channel impulse response seen by Bob and $\mathbf{z}_b$ represents additive white Gaussian noise (AWGN) at Bob with distribution of $\mathcal{CN}(0, N_{0,T})$. Similarly, the baseband signal received at Eve is given by:

$$\mathbf{y}_e = \mathbf{h}_e * \tilde{\mathbf{q}} + \mathbf{z}_e, \tag{6.10}$$

where $\mathbf{h}_e$ is the channel impulse response seen by Eve and $\mathbf{z}_e$ represents AWGN at Eve with distribution of $\mathcal{CN}(0, N_{0,TE})$.

The basic block diagram of the receiver is presented in Fig. 6.3. The receiver (both Bob and Eve) first removes the CP and then applies FFT on the received time domain signal $\mathbf{y}_d$ with normalization factor of $\frac{K}{\sqrt{N}}$ and finally deinterleaves the resultant signal to get the received signal, $\mathbf{y}_{fd} = [y_{fd}(1), y_{fd}(2), ..., y_{fd}(N)]^T$, in frequency domain, where d can be Bob or Eve.

The receiver task is to detect the indices of active subcarriers and corresponding symbols by processing, $y_{fd}(\alpha)$, where $\alpha = \{1, ..., N\}$. In our algorithm, we use look up table based modified Log-likelihood-Ratio (LLR) detector for detection of active indices for each subblock [114]. First of all, LLR values of frequency domain symbols corresponding to each subcarrier are calculated as follows:

$$\lambda(\alpha) = \ln\left(\frac{\sum_{\chi=1}^{M} P(x(\alpha) = s_\chi \mid y_{fd}(\alpha))}{P(x(\alpha) = 0 \mid y_{fd}(\alpha))}\right) \tag{6.11}$$

The above equation can be further simplified by using Bayes' formula as

$$\begin{aligned}\lambda(\alpha) = \ln(k) - \ln(n-k) + \frac{\mid y_{fd}(\alpha) \mid^2}{N_{0,f}} \\ + \ln\left(\sum_{\chi=1}^{M} exp\Big(-\frac{1}{N_{0,f}} \mid y_{fd}(\alpha) - h_F(\alpha)s_\chi \mid^2\Big)\right)\end{aligned} \tag{6.12}$$

where $N_{0,f}$ is the noise variance in frequency domain ($N_{0,f} = (K/N)N_{0,T}$). In (12), numerical overflow can be prevented by using the Jacobian logarithm [134] . For example, for $M = 2$ and $k_j = n/2$, (12) simplifies to

$$\lambda(\alpha) = max(a, b) + \ln(1 + exp(- \mid b - a \mid)) + \frac{\mid y_{fd}(\alpha) \mid^2}{N_{0,f}} \tag{6.13}$$

where $b = - \mid y_{fd}(\alpha) + h_f(\alpha) \mid^2 / N_{0,f}$ and $a = - \mid y_{fd}(\alpha) - h_f(\alpha) \mid^2 / N_{0,f}$. In our work, we also use higher order modulation and use the following identity $\ln(e^{a_1} + e^{a_1} + ... + e^{a_M}) = (f_{max}(f_{max}(...f_{max}(f_{max}(a_1, a_2), a_3), ...), a_M))$, where $f_{max}(a, b) = \ln(e^{a_1} + e^{a_1}) = max(a_1, a_2) + \ln(1 + e^{-|a_1 - a_2|})$.

In order to detect the active indices, LLR value corresponding to each subcarrier is calculated using (12). Afterwards, the receiver calculates the sum of LLRs corresponding to each combination of the subcarriers in the lookup table with respect to subblock based SAR as follows:

$$d_\beta^w = \sum_{\gamma=1}^{k_j} \lambda(n(\beta - 1) + i_{\beta,\gamma}^w) \tag{6.14}$$

where $w = 1, ..., c$ and c is the total number of combinations of subcarriers in the look up table with respect to any SAR. The receiver makes a decision of set of active indices by selecting the set with maximum value of sum of LLRs as follows:

$$\hat{w} = arg \max_w d_\beta^w \tag{6.15}$$

After selecting the set with maximum LLR, the receiver gets the set of active indices corresponding to SAR. After the detection of active subcarrier, the information is then passed to index demapper based on look-up table to estimate m_{1i} bits. After determination of active indices, the demodulation of the constellation symbols (M-ary symbols) is carried out and finally we get m_{2i} bits.

6.3.2 Proposed Algorithms for OFDM-IM

In this subsection, proposed algorithms for enhancing PLS and spectral efficiency are presented.

6.3.2.1 OFDM-AIM-FCM

In OFDM-AIM-FCM, SAR for each subblock is changed adaptively while fixed CM is used for all subblocks. The basic idea of OFDM-AIM-FCM is presented in Fig. 6.5. The basic steps for OFDM-AIM-FCM algorithm are as follows:

SAR: [1/4]

Bits	Subcarrier indices
00	1
01	2
10	3
11	4

SAR: [2/4]

Bits	Subcarrier indices
00	1, 2
01	2, 3
10	3, 4
11	1, 4

SAR: [3/4]

Bits	Subcarrier indices
00	1,2,3
01	1,2,4
10	1,3,4
11	2,3,4

Fig. 6.4: Look up table for SAR values of $\{1/4, 2/4, 3/4\}$.

- In the first step, the channel is estimated at all nodes. In order to do that, Alice and Bob send a reference signal to each other (within coherence time). After channel estimation, they take FFT to convert the channel coefficient vector into frequency domain vector, $\mathbf{h}_f$.

- Afterwards, the vector $\mathbf{h}_f$ at each node is divided into G subblocks with n elements in each of, β, subblock, where $n = N/G$.

- In the next step, the average, $av(\beta)$, of absolute values of subblock's elements is calculated as follows

$$av(\beta) = \frac{\sum_{r=1}^{n} \mid hs_{\beta,r} \mid}{n}, \tag{6.16}$$

  where $hs_{\beta,r}$ is the r_{th} element of β subblock.

- After finding the average value, $av(\beta)$, for each of G subblocks, they are divided into four groups based on their $av(\beta)$. More specifically, find the mean, me, of $\mathbf{av}$, where $\mathbf{av}$ is a vector containing average values for all subblocks. Afterwards, divide the subblocks into two groups, $\mathbf{g}_1$ and $\mathbf{g}_2$, by comparing their corresponding $av(\beta)$ values with me. The sub-group $\mathbf{g}_1$ contains those subblocks whose $av(\beta)$ values are greater than or equal to

me while $\mathbf{g}_2$ contains those subblocks whose values of $av(\beta)$ are less than me. Afterwards, both $\mathbf{g}_1$ and $\mathbf{g}_2$ are further divided into two sub-groups by using mean method as explained above. As a result, G subblocks are divided into four groups such as $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$ and $\mathbf{g}_{44}$. The resultant groups are sorted in descending order in term of average channel magnitude such that $\mathbf{g}_{11}$ contains those subblocks that have highest values of $av(\beta)$ while $\mathbf{g}_{44}$ contains subblocks with lowest values of $av(\beta)$.

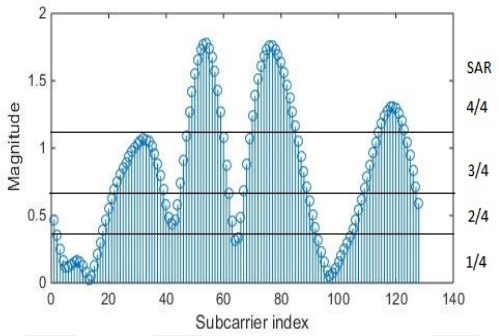


Fig. 6.5: Proposed: OFDM-IM-AIM-FCM.

Table 6.1: OFDM-AIM-FCM.

Group	SAR
$\mathbf{g}_{11}$	4/4
$\mathbf{g}_{22}$	3/4
$\mathbf{g}_{33}$	2/4
$\mathbf{g}_{44}$	1/4

- Finally, higher SAR values are selected for those groups that have higher values of $av(\beta)$ while lower values of SAR are selected for those groups that have lower values of $av(\beta)$, such that SAR values of 4/4, 3/4 , 2/4 and 1/4 are selected for groups $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$ and $\mathbf{g}_{44}$, respectively, as presented in Table 6.1.

Based on the above algorithm (OFDM-AIM-FCM), Alice determine SAR for each subblock and the total number of bits, m_i, for i_{th} block. Afterwards, data is

loaded to the indices and the symbols based on adaptive SAR and fixed CM and a block is generated using adaptive OFDM-IM model explained in subsection III.A. Finally, the resultant signal $\tilde{\mathbf{q}} \in C^{[N+L\times 1]}$ is transmitted through the Rayleigh fading channel and reaches to both Bob and Eve.

Bob and Eve will then detect the active subcarriers based on SAR values of subblocks with respect to OFDM-AIM-FCM. The resultant information is passed to the index demapper that provides the information carried by indices. After determination of active indices, constellation symbols are demodulated.

Thanks to channel decorrelation assumptions, Bob and Eve will have differences in their determined subblock based SAR values. Due to channel reciprocity employment, the SAR values for different subblocks determined by Bob are similar to that of Alice's while they are different at Eve. This dissimilarity in SAR values for different subblocks at Eve leads to wrong detection of bits at Eve. Hence, there is a performance gap at Bob and Eve, which enables the secure communication between Alice and Bob.

6.3.2.2 OFDM-AIM-ACM

In OFDM-AIM-ACM both the SAR and CM order are adaptively varied based on channel of legitimate node in order to enhance PLS and SE. The basic concept of OFDM-AIM-ACM is presented in Fig. 6.6.

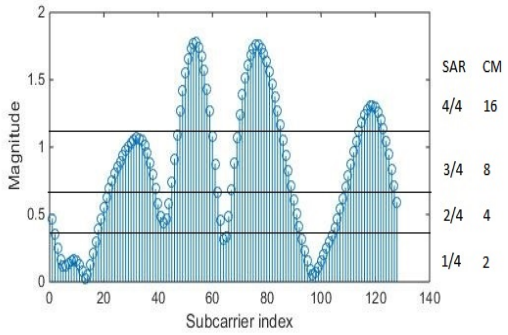


Fig. 6.6: Proposed: OFDM-AIM-ACM

Table 6.2: OFDM-AIM-ACM

Group	SAR	M
$\mathbf{g}_{11}$	4/4	16
$\mathbf{g}_{22}$	3/4	8
$\mathbf{g}_{33}$	2/4	4
$\mathbf{g}_{44}$	1/4	2

- First four steps of OFDM-AIM-ACM are similar to that of OFDM-AIM-FCM. Specifically, $\mathbf{h}_f$ vector is divided into G subblocks. The resultant G subblocks are grouped into four groups such as $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$ and $\mathbf{g}_{44}$ using mean method as explained earlier.

- The basic difference in OFDM-AIM-ACM as compared to OFDM-AIM-FCM is that both the SAR and CM order are varied adaptively for each subblock in it. In OFDM-AIM-ACM, higher SAR with higher order CM are selected for those groups that have high values of $av(\beta)$ while lower values of SAR with lower order CM are selected for those groups that have lower values of $av(\beta)$. Based on OFDM-AIM-ACM, SAR value of 4/4 is selected with $M = 16$, 3/4 with 8, 2/4 with 4 and 1/4 with 2 for groups $\mathbf{g}_{11}$, $\mathbf{g}_{22}$, $\mathbf{g}_{33}$ and $\mathbf{g}_{44}$, respectively, as presented in Table. 6.2.

Based on the above mentioned algorithm (OFDM-AIM-ACM), Alice determine SAR and CM order for each subblock and the total number of bits, m_i, for i_{th} block. Afterwards, data is loaded to the indices and symbols based on adaptive SAR and adaptive CM and finally a block is generated using adaptive OFDM-IM model explained in subsection III.A. Finally, the resultant signal $\tilde{\mathbf{q}} \in C^{[N+L\times 1]}$ is transmitted through the Rayleigh fading channel and reaches to both Bob and Eve.

Bob and Eve will first detect active subcarriers based on subblock-SAR values with respect to OFDM-AIM-ACM. The resultant information is then passed to the index demapper which provides the information carried by indices. After determination of active indices, constellation symbols are demodulated based on

subblock CM order with respect to OFDM-AIM-ACM.

Due to the channel decorrelation, the SAR values and CM orders of different subblocks determined by Bob and Eve based on OFDM-AIM-ACM are different. The SAR values and CM orders of different subblock determined by Bob is similar to that of Alice's due to channel reciprocity, while it is different at Eve as compared to Alice. This difference in subblock based SAR values as well as CM order at Eve compared to Alice will cause errors in the detection of data carried by indices and symbols. Hence, there is a significant performance gap between Bob and Eve. This performance gap will ensures secure communication between Alice and Bob. It should also be noted that OFDM-AIM-ACM is more difficult to be attacked as compared to OFDM-AIM-FCM because in the latter case only subblock based SAR is varied adaptively, while in the former both the SAR and CM are varied adaptively.

6.3.2.3 OFDM-VIM-VCM for QoS

In OFDM-VIM-VCM, the IM and CM order are varied for QoS based communication in order to maximize the spectral efficiency. The basic motivation behind this approach is that instead of using complex optimization based approaches for maximizing spectral efficiency, simple simulation based approach is proposed for this purpose. The basic concept is to vary the SAR and CM with the change in average SNR to maximize the spectral efficiency while fulfilling certain QoS requirement. The basic procedure can be summarized as follows:

- First, OFDM-IM is implemented with different modulation order for each SAR. Afterwards, BER and Throughput curves are simulated for each of SAR value with higher order modulation, for example, in this work, we are considering SAR values of 1/4, 2/4, 3/4 and 4/4 and CM order of 2, 4, 8 and 16.
- Then, all BER curves are merged in one figure and all throughput curves in another figure.

- In the next step, certain BER curves are selected based on their performance gap and throughput values. More specifically, among the BER curves that have similar performance, select a curve that has maximum value of throughput. From the selected curves in the former step, select those curves that have a performance gap between them. Afterwards, the throughput curves corresponding to selected BER curves are also selected.
- Finally, switching table is constructed based on QoS requirement. The table depicts the values of different SAR and CM of system for different average SNR ranges to maximize the spectral efficiency while fulfilling QoS requirements.
- After construction of switching table, this table is then used for QoS based communication for maximizing spectral efficiency.

6.4 Performance Analysis of Adaptive OFDM-IM Scheme

6.4.1 Throughput of Adaptive OFDM-IM

This section presents the details related to the throughput of the adaptive OFDM-IM. The throughput for adaptive OFDM-IM can be given as

$$Throughput = \frac{\sum_{j=1}^{G} p_{1j} + \sum_{j=1}^{G} p_{2j}}{N + N_{CP}} \tag{6.17}$$

where $p_{1j} = \lfloor \log_2 \binom{n}{k_j} \rfloor$ and $p_{2j} = k_j \log_2 M_j$. The basic difference between conventional OFDM-IM and adaptive OFDM-IM is in k_j and M_j which are fixed in the former but vary adaptively in the latter. In case of OFDM-ACM-FCM, k_j is different for different subblocks and M_j is same for all subblocks while in case of OFDM-ACM-AIM and OFDM-VIM-VCM both k_j and M_j are different for different subblocks.

6.4.2 Performance Analysis of Adaptive OFDM-IM Scheme

This section presents the analytical evaluation for the upper bound of the average bit error probability (ABEP) of the adaptive OFDM-IM scheme (OFDM-AIM-FCM with $M = 2$) based on pairwise error probability (PEP). In this analysis, ML detector with a look-up table is considered whose results are equal to and applicable to the modified LLR detector (near ML) with a look up table. This is because of the fact that the error performance of ML detector is almost similar to that of modified LLR detector as explained in [114].

In the conventional OFDM-IM, same SAR value are used in all subblocks while in case of OFDM-AIM-FCM different SARs values are used in different subblocks. As explained earlier that there are N subcarriers that are divided into G subblocks with n subcarriers in each subblock. In OFDM-AIM-FCM, the subblocks are divided into four groups, $\mathbf{g_{44}}$, $\mathbf{g_{33}}$, $\mathbf{g_{22}}$ and $\mathbf{g_{11}}$ with SAR values of 1/4, 2/4, 3/4, and 4/4, respectively, used in them. In order to simplify the analysis, we can assume that the size of each of above mentioned groups in OFDM-AIM-FCM is same.It should be noted that the PEP event is similar in the subblocks corresponding to the same group and is different for subblocks that belong to different groups.

In the first step, the average bit error probability (ABEP) of first subblock of first group is calculated and then the results are extended to include subblocks of other groups. Afterwards, we will find average ABEP for each group and finally find the ABEP of adaptive OFDM-IM subblock.

The input output relationship in frequency domain for the first subblock of first group is given as:

$$\mathbf{y} = \mathbf{X}\mathbf{h} + \mathbf{w}. \tag{6.18}$$

where $\mathbf{X}$ is an $n \times n$ diagonal matrix containing $[x(1), x(2), \ldots, x(n)]^T$

as diagonal data elements, $\mathbf{y}$ is the received signal sub-vector containing $[y_{fd}(1), y_{fd}(2), \ldots, y_{fd}(n)]^T$, $\mathbf{h}$ is the channel sub-vector containing $[h_f(1), h_f(2), \ldots, h_f(n)]^T$ and $\mathbf{w}$ is the noise sub-vector containing $[w(1), w(2), \ldots, w(n)]^T$. Let us assume that $\mathbf{K_n} = E[\mathbf{h}\mathbf{h}^H]$ is a covariance sub-matrix of rank r_1 ($r_1 = rank(\mathbf{K_n})$).This matrix is valid for all subblocks. Moreover, the concatenation of these small covariance sub-matrices give $\mathbf{K}$ matrix which is the covariance matrix of $\mathbf{h}_f$. Let us suppose that $\mathbf{X}$ signal is transmit-

Table 6.3: System parameters.

Channel	Multipath Rayleigh fading channel
Channel length	10
OFDM frame size (N)	128
Length of subblock	4
Detector	Modified LLR based detector

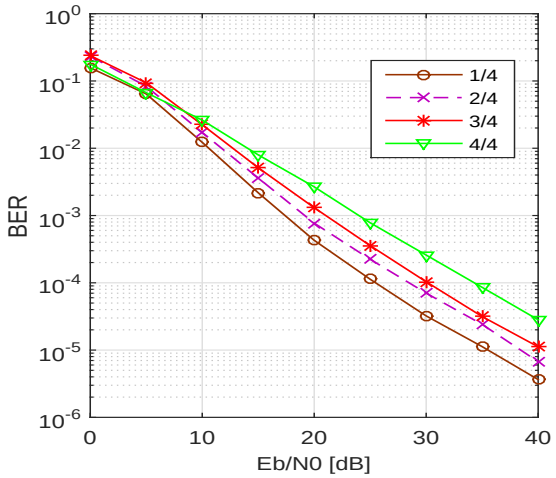


Fig. 6.7: BER performance for OFDM-IM ($n = 4$, $k = \{1, 2, 3, 4\}$).

ted through channel and received as erroneous signal $\hat{\mathbf{X}}$. The receiver can make decision error in both constellation symbols and indices. One of the best way to analyse these error is in terms of PEP. In [135], an expression for conditional pairwise error probability (CPEP) is presented for the model of (18) and is given

as

$$P(\mathbf{X} \longrightarrow \hat{\mathbf{X}}|\mathbf{h}) = Q\left(\sqrt{\frac{\delta}{2N_{0,f}}}\right), \tag{6.19}$$

where $\delta = \mathbf{h^H A h}$, and the $\mathbf{A}$ matrix equals to $(\mathbf{X}-\hat{\mathbf{X}})^H(\mathbf{X}-\hat{\mathbf{X}})$. In order to find the unconditional pairwise error probability (UPEP), the expectation of CPEP is taken with respect to the channel and is given as: $P(\mathbf{X} \longrightarrow \hat{\mathbf{X}}) = E_h\{Q(x)\}$. Based on [136], we can define an orthogonal matrix $\mathbf{F}$ where $\mathbf{F^H F} = \mathbf{I}$. The covariance sub-matrix and channel can be simplified as $\mathbf{K_n} = \mathbf{F D F^H}$ and $\mathbf{h} = \mathbf{F u}$, respectively. Here, $\mathbf{D}$ is a diagonal matrix and is equal to $\mathbf{D} = E[\mathbf{u u^H}] = \mathbf{D}$ and $\mathbf{u}$ is eigen vector. Using the probability density function (p.d.f) of $\mathbf{u}$ [114] and simplification of $Q(x)$ and δ, the Unconditional Pairwise Error Probability (UPEP) can be written as

$$P(\mathbf{X} \longrightarrow \hat{\mathbf{X}}) = \frac{1/12}{det(\mathbf{I_n} + q_1\mathbf{B})} + \frac{1/4}{det(\mathbf{I_n} + q_2\mathbf{B})}, \tag{6.20}$$

where $\mathbf{I_n}$ is an identity matrix, $\mathbf{B} = \mathbf{A K_n}$, $q_1 = 1/(4N_{0,f})$ and $q_2 = 1/(3N_{0,f})$. The above equation can be further simplified as:

$$P(\mathbf{X} \longrightarrow \hat{\mathbf{X}}) = (12q_1^r \prod_{\xi=1}^{r} \lambda_\xi(B))^{-1} + (4q_2^r \prod_{\xi=1}^{r} \lambda_\xi(B))^{-1} \tag{6.21}$$

where $r \leq min\{r_1, r_2\}$ and $r_2 = rank(A)$. For different SAR r_2 will be different, so above equation (21) is still applicable to any SAR.

The overall average bit error probability of τ_{th} subblock of any group can be calculated by using UPEP as follows:

$$\begin{aligned} P_b^\tau(E) \;\; &\approx \tfrac{1}{p^\tau\, n_x^\tau} \textstyle\sum_{\mathbf{X}^\tau} \sum_{\hat{\mathbf{X}}^\tau} P(\mathbf{X}^\tau \longrightarrow \hat{\mathbf{X}}^\tau) \\ &\qquad e(\mathbf{X}^\tau, \hat{\mathbf{X}}^\tau), \end{aligned} \tag{6.22}$$

where p^τ is the number of information bits in τ_{th} subblock of any group, n_x^τ represents the number of realizations of $\mathbf{X}^\tau$, and $e(\mathbf{X}^\tau, \hat{\mathbf{X}}^\tau)$ is the number of information bit errors committed by choosing $\hat{\mathbf{X}}^\tau$ instead of $\mathbf{X}^\tau$. Using the above equation (22), the ABEP for Υ_{th} group can be calculated as:

$$P_b^{\Upsilon}(E) \approx \frac{1}{F}\Big(\sum_{\tau=1}^{F} P_b^{\tau}(E)\Big) \tag{6.23}$$

where F is the number of subblocks in any group and $F = 8$ in our case. Equation (23) can be re-written as:

$$\begin{aligned} P_b^{\Upsilon}(E) \;\approx \tfrac{1}{F}\textstyle\sum_{\tau=1}^{F}\Big(\tfrac{1}{p^{\tau}\, n_x^{\tau}}\sum_{\mathbf{X}^{\tau}}\sum_{\hat{\mathbf{X}}^{\tau}} P(\mathbf{X}^{\tau} \longrightarrow \hat{\mathbf{X}}^{\tau}) \\ e(\mathbf{X}^{\tau}, \hat{\mathbf{X}}^{\tau})\Big) \end{aligned} \tag{6.24}$$

Finally, ABEP for the OFDM-IM block can be calculated as follows:

$$P_b(E) \approx \frac{1}{\Omega}\sum_{\Upsilon=1}^{\Omega} P_b^{\Upsilon}(E) \approx \frac{1}{\Omega}\Big(P_b^1 + P_b^2 + P_b^3 + P_b^4\Big) \tag{6.25}$$

where Ω is the number of groups and in this case $\Omega = 4$. The theoretical BER curve will be presented Section V.

6.5 Simulation Result

This section presents the simulation results to evaluate the effectiveness of the proposed algorithms, named as OFDM-AIM-FCM, OFDM-AIM-ACM and OFDM-VIM-VCM by using bit error rate (BER) and throughput as performance metrics.

In this work, we consider an OFDM-IM system with $N = 128$ subcarriers and a CP of length 10. As explained in subsection III.A, OFDM-IM block is divided into $G = N/n = 128/4 = 32$ subblocks, where $n = 4$ is the number of subcarriers in each subblock. The multi-path Rayleigh fading channel is considered for both Bob and Eve with equal number of channel taps ($L = 10$). The basic simulation parameters are presented in Table. 6.3. In this work, look-up table based special

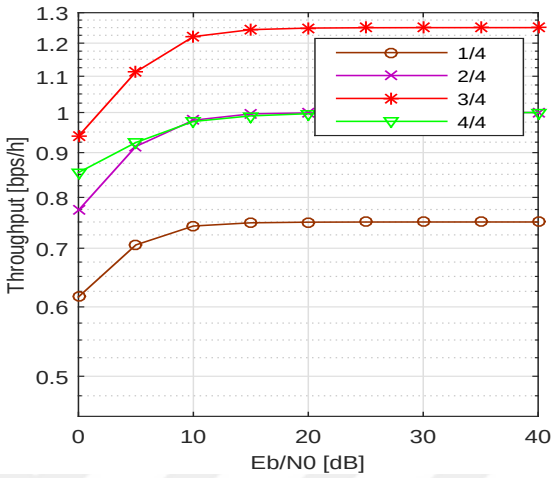


Fig. 6.8: Throughput performance for OFDM-IM ($n = 4$, $k = \{1, 2, 3, 4\}$).

LLR detector is employed at receiver, as explained in subsection III.A, to determine the active indices and corresponding constellation symbols based on the proposed algorithms. Additionally, we also consider that Eve knows our security algorithms. For simplicity and without loss of generality, CP is not considered in the throughput calculation.

It should be noted that the proposed scheme is a type of scheme which does not cause much difference in the SNR between Bob and Eve, but still Eve cannot decode, while Bob can decode (This case is somehow similar to the case of interleaver or precoder based security techniques [137], [138]). In such cases, BER can be used as a metric to measure secrecy instead of secrecy capacity and secrecy outage probability as reported in [137], [138], [139]. Therefore, in this work, we use BER-based secrecy gap metric [138] to evaluate the secrecy. Furthermore, in this work we are targeting Quality of service (QoS) based security [124]. The basic idea behind QoS based security is to secure different services (voice, video etc) instead of focusing on providing perfect secrecy. More specifically, it should be noted 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. So, in this work we target to provide security for services such as voice and video and make sure that error rate at Eve is greater

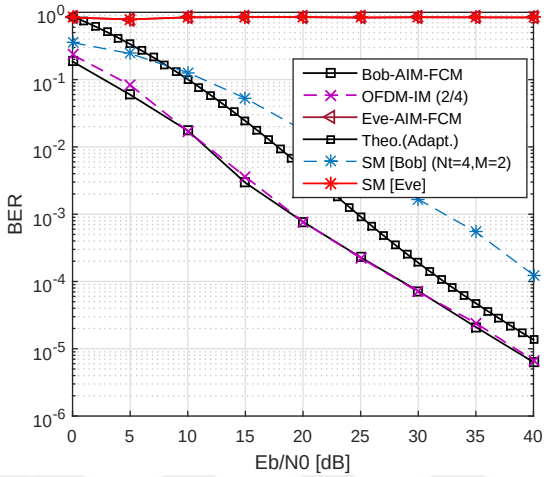


Fig. 6.9: BER performance for OFDM-AIM-FCM, Secure SM [3] and OFDM-IM $(n = 4, k = 2)$.

than minimum required error rate criteria to use that service [124]. For example, voice and video can be made secure at Bob by making sure that PER (corresponding to BER) at Bob is less than minimum required PER (corresponding to BER) in order to use that service while PER at Eve is made greater than minimum required PER. The minimum PER requirement for different services are presented in Table 6.4 [6]. Hence, although the throughput is non-zero, the proposed scheme can still provide QoS based security (It should be noted that PER can be calculated from BER as follows: $PER = 1 - (1 - BER)^n$), where n is the block size).

Table 6.4: QoS LOOKUP TABLE [6].

Service	PER
Voice	10^{-2}
Video	10^{-3}

In the first phase, OFDM-IM is simulated for different SAR values, such as 1/4, 2/4, 3/4 and 4/4 based on lookup tables presented in Fig. 6.4 with FCM (M=2). Afterwards, we simulate OFDM-AIM-FCM for BPSK ($M = 2$) for PLS and also extend it for higher order modulation such as $M = 4$, $M = 8$ and $M = 16$. Then, OFDM-AIM-FCM is extended to OFDM-AIM-ACM for providing another

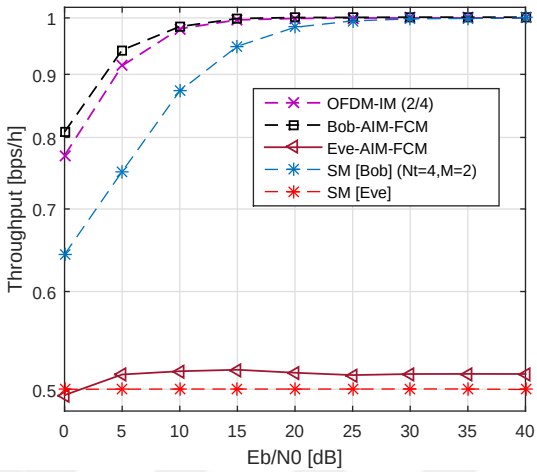


Fig. 6.10: Throughput performance for OFDM-AIM-FCM, Secure SM [3] and OFDM-IM $(n = 4, k = 2)$.

stronger PLS technique. Finally, we implement OFDM-VIM-VCM for QoS based communication in order to maximize the spectral efficiency.

6.5.1 OFDM-AIM-FCM

Fig. 6.7 presents the BER plots for OFDM-IM with different SAR values, such as 1/4, 2/4, 3/4 and 4/4 for $M = 2$. It should be noted from Fig. 6.7 that the BER performance for lower values of SAR is better than the case of higher values of SAR, for example, the BER performance of 1/4 case is best while BER performance of 4/4 is worst. The reason for the better performance of BER at lower SAR is due to the fact that in case of lower SAR there will be less noise in the frequency domain.

Fig. 6.8 presents throughput for OFDM-IM with different SAR values for $M = 2$. It should be noted that the throughput for the system improves as the activation ratio increases except for the case with SAR value of 3/4 which outperform 4/4 case. The reason is that each subblock carries 4 bits in case of SAR value of 4/4 while each block carries 5 bits in case of 3/4.

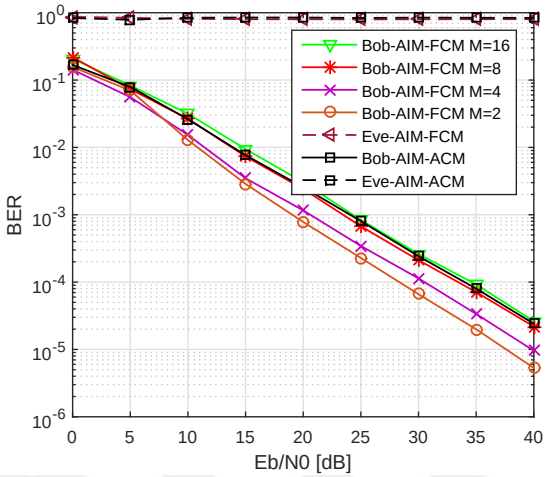


Fig. 6.11: BER performance for OFDM-AIM-FCM and OFDM-AIM-ACM.

Fig. 6.9 presents a comparison of BER performances among the proposed OFDM-AIM-FCM scheme, the scheme presented in [3] and OFDM-IM ($n = 4, k = 2$) (Ref.[1]). It is observed from Fig. 6.9 that the BER performances of OFDM-AIM-FCM and OFDM-IM [114] are similar for the case of Bob but the scheme presented in [3] have worst performance as compared to others. It is also observed that the performance of Eve is worst for all values of SNR for the proposed OFDM-AIM-FCM technique and the scheme presented in [3] while her performance is similar to that of Bob for the cases of OFDM-IM [114]. Hence, the proposed technique and the technique presented in [3] are secure as compared to OFDM-IM [114]. Fig. 6.9 also presents the theoretical upper bound BER performance of OFDM-AIM-FCM based on (25). It should be noted that theoretical curve becomes tight at higher SNR with the simulation curve.

Fig. 6.10 shows the comparison of throughput performances among the proposed OFDM-AIM-FCM scheme, the scheme presented [3] and OFDM-IM ($n = 4, k = 2$) [114] with $M = 2$. It is observed that the throughput performances of all of these schemes for Bob are approximately similar at higher values of SNR. At equivalent BER we can notice that the throughput of the proposed OFDM-AIM-FCM scheme outperforms the OFDM-IM (2/4) [114] at lower values of SNR. Moreover, the proposed scheme (OFDM-AIM-FCM) also outperforms in

[1]Ref. means the reference scheme to which we compare our proposed algorithm.

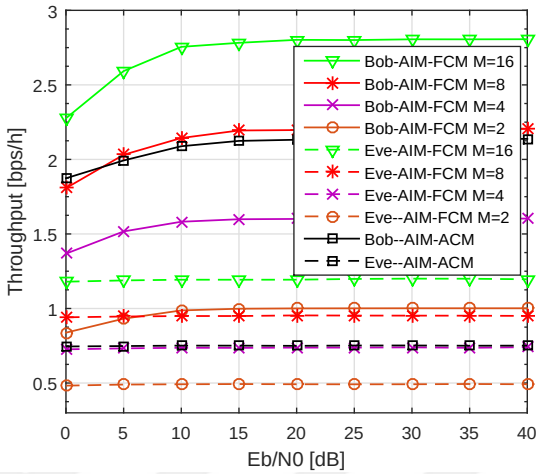


Fig. 6.12: Throughput performance for OFDM-AIM-FCM and OFDM-AIM-ACM.

terms of throughput as compared to the scheme presented [3] at lower values of SNR. It is also observed that the throughput performance of Eve is worst for the proposed OFDM-AIM-FCM technique and the scheme presented in [3] while her performance is similar to that of Bob for the case of OFDM-IM [114] scheme.

6.5.2 OFDM-AIM-ACM

Fig. 6.11 presents the BER performance of Bob and Eve for OFDM-AIM-FCM for $M = 2$, $M = 4$, $M = 8$, and $M = 16$. It should be noted from the figure that as the modulation order increases the BER performance degrades. The performance of Eve for OFDM-AIM-FCM is worst for all cases of CM such as $M = 2$, $M = 4$, $M = 8$, and $M = 16$. Fig. 6.11 also presents the BER performance of Bob and Eve for the proposed OFDM-AIM-ACM. It is observed from Fig. 6.11 that the BER performance of OFDM-AIM-AIM is approximately same as the case of OFDM-AIM-FCM for $M = 8$, while the BER performance of Eve is worst for all values of SNR. Hence, OFDM-AIM-ACM can provide secure communication between Alice and Bob. Fig. 6.12 presents throughput performance of Bob and Eve for OFDM-AIM-FCM with $M = 2$, $M = 4$, $M = 8$ and $M = 16$. Similarly,

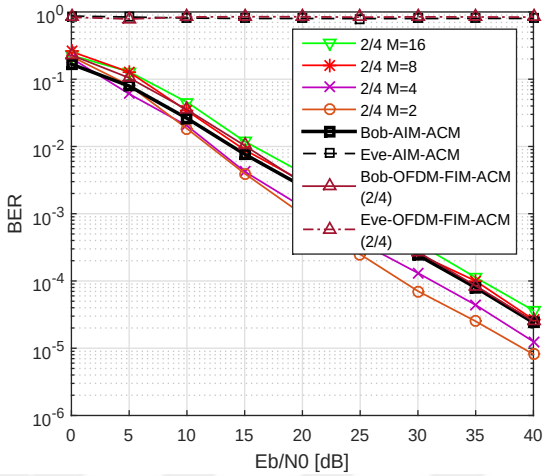


Fig. 6.13: BER comparison of OFDM-IM $(n = 4, k = 2)$, OFDM-AIM-ACM and OFDM-FIM-ACM $(n = 4, k = 2)$.

Fig. 6.12. also presents the throughput results of our proposed OFDM-AIM-ACM based PLS technique for Bob and Eve. It is clear from Fig. 6.12 that the throughput of OFDM-AIM-ACM is approximately similar to the case of OFDM-AIM-FCM with $M = 8$ while throughput of Eve is worst for all the values of SNR.

Fig. 6.13 presents a comparison of BER performances between the proposed OFDM-AIM-ACM scheme and OFDM-IM $(n = 4, k = 2)$ (Ref.) with CM order of {2,4,8,16}. It is observed from Fig. 6.13 that the BER performance of OFDM-AIM-ACM is similar to the case of OFDM-IM $(n = 4, k = 2)$ (Ref.) with $M = 8$. At equivalent BER, it is also noticed that the throughput of the proposed OFDM-AIM-ACM outperforms the OFDM-IM $(n = 4, k = 2)$ (Ref.) with $M = 8$ at all values of SNR as presented Fig. 6.14. It is also observed from Fig. 6.13 and Fig. 6.14 that the BER and throughput performances of Eve are worst at all values of SNR for the proposed OFDM-AIM-ACM scheme while her BER and throughput performances are similar to that of Bob for the cases of OFDM-IM $(n = 4, k = 2)$ (Ref.). Hence, the proposed scheme can enhance security and spectral efficiency jointly.

Moreover, Fig. 6.13 and Fig. 6.14, respectively, compare the BER and

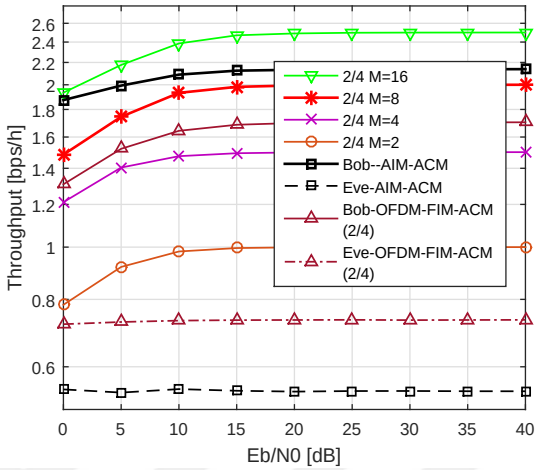


Fig. 6.14: Throughput comparison of OFDM-IM ($n = 4, k = 2$), OFDM-AIM-ACM and OFDM-FIM-ACM ($n = 4, k = 2$).

throughput performances of the OFDM-AIM-ACM scheme with the OFDM-FIM-ACM ($n = 4, k = 2$) based on [140]. It is observed from the figures that at approximately equivalent BER the proposed OFDM-AIM-ACM outperforms OFDM-FIM-ACM ($n = 4, k = 2$) in terms of throughput. It is also observed from Fig. 6.13 and Fig. 6.14 that OFDM-FIM-ACM ($n = 4, k = 2$) can also provide security. Note that OFDM-AIM-ACM is more secure as compared to OFDM-AIM-FCM because in the case of OFDM-AIM-ACM both SAR and CM are varied adaptively while in case of OFDM-AIM-FCM only SAR is varied.

The below sub-sections present the effect of imperfect channel estimation and effect of channel correlation between Bob's channel and Eve's channel on the performances of OFDM-AIM-FCM and OFDM-AIM-ACM.

6.5.2.1 Security Algortihms under imperfect channel estimation

In order to evaluate the robustness of the the proposed security algorithms against imperfect channel estimation, intentional error is added at both the transmitter

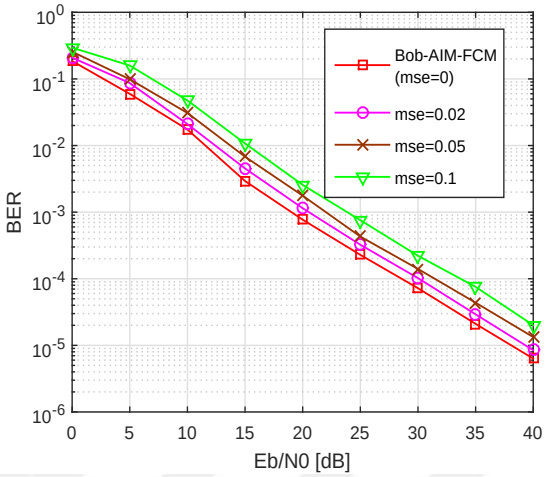


Fig. 6.15: BER comparison of OFDM-AIM-FCM ($mse = 0, 0.02, 0.05, 0.1$).

and receiver ($\Delta\mathbf{h}_{T/R}$) to the true channel ($\mathbf{h}$) to obtain new erroneous channels given by $\tilde{\mathbf{h}} = \mathbf{h} + \Delta\mathbf{h}$ [138] [141] . The intentional error ($\Delta\mathbf{h}$) is modeled as an independent complex Gaussian noise with zero mean and variance ($\sigma^2 = mse \times 10^{\frac{-SNR_{dB}}{10}}$), where mse is a variable related to mean square of estimator's quality. Fig .15 and Fig. 6.16, respectively, present the BER performances for OFDM-AIM-FCM and OFDM-AIM-ACM under different estimation qualities with $mse = 0$ (perfect estimation), $mse = 0.02$, $mse = 0.05$ and $mse = 0.1$. It is shown that imperfect channel estimation leads to small degradation in the BER performance. However, this degradation can be overcome by increasing the length or power of the training sequence. Moreover, there are some interesting algorithms proposed in the literature that can minimize the channel estimation error, such as in [109]

6.5.2.2 Effect of Eve's channel correlation with Bob's channel

This subsection presents the effect of the correlation between the channel of legitimate receiver and Eve and evaluate the performance in term of BER as a security metric. Firstly, the assumption of channel decorrelation requires that Bob and Eve be located at more than one-half-wavelength away from Alice. This is a practical assumption in many realistic scenarios and is assumed in many

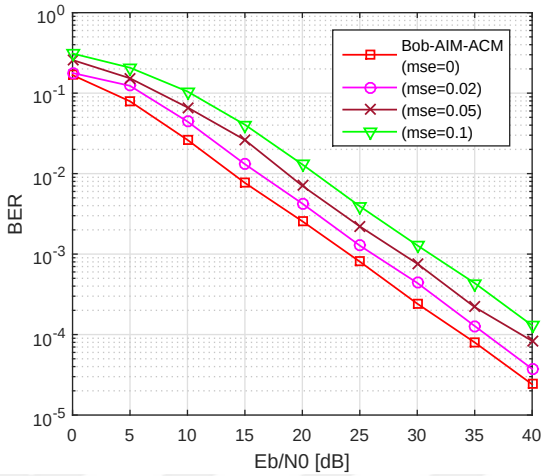


Fig. 6.16: BER comparison of OFDM-AIM-ACM ($mse = 0, 0.02, 0.05, 0.1$).

prominent works in the literature (such as [142] [143] [144]). We have performed additional new simulations to show the effect of the correlation between the channel of legitimate receiver and eavesdropper on the secrecy performance measured in term of BER as a security metric as explained above.

Fig. 6.17 and Fig. 6.18, respectively, present the BER performances for OFDM-AIM-FCM and OFDM-AIM-ACM when Eve's channel is correlated to Bob's one. The model for channel correlation assumed in this work is similar to the one presented in [144] and is given as follows:

$$h_e = \rho h_b + (1 - \rho)E \tag{6.26}$$

where E represents an independent channel while ρ is the correlation factor. We present BER performance for the correlation values of ($\rho = 0, 0.80, 0.90, 0.95, 0.99$). It should be noted that even with correlation between Bob's and Eve's channels, the proposed algorithms can still provide some level of QoS based security.

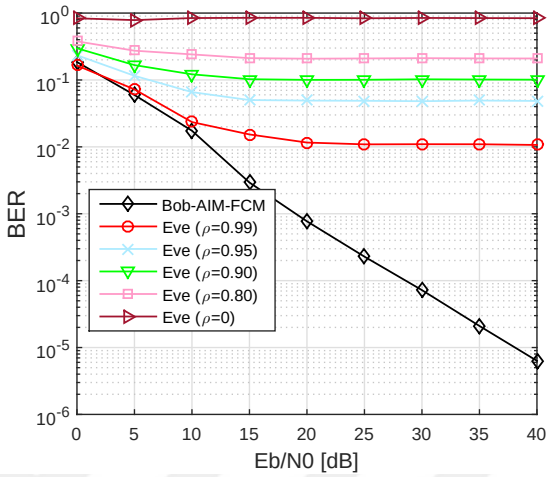


Fig. 6.17: BER comparison of Bob (OFDM-AIM-FCM) and Eve with correlation coefficient ($\rho = 0, 0.80, 0.90, 0.95, 0.99$).

6.5.3 OFDM-VIM-VCM

Fig. 6.19 and Fig. 6.20 present the extensive simulations related to OFDM-VIM-VCM scheme for QoS based communication in order to maximize the spectral efficiency. Note that the system model for this technique is the same as explained in Section II, except the Eve link, which is not considered in this case. The basic concept is to vary the SAR and CM with the increase in SNR to maximize the spectral efficiency while fulfilling certain QoS requirement. In this approach, BER and throughput curves for four types of CM order, such as $M = 2$, $M = 4$, $M = 8$, and $M = 16$ are implemented for each of SAR type such as, 1/4, 2/4, 3/4 and 4/4 and presented in Fig. 6.19, Fig. 6.20. a and Fig. 6.20. d. Afterwards, certain curves are selected based on OFDM-VIM-VCM for QoS based communication.

In Fig. 6.20. b, we merge the BER curves of SAR values of 1/4, 2/4, 3/4 and 4/4 for CM order of $M = 2$, $M = 4$, $M = 8$, and $M = 16$. Similarly, in Fig. 6.20. e, throughput curves of SAR values of 1/4, 2/4, 3/4 and 4/4 for CM order of $M = 2$, $M = 4$, $M = 8$, and $M = 16$ are also merged.

Afterwards, among the BER curves of Fig. 6.20. b that have similar performance, we select a curve that has maximum value of throughput. From the

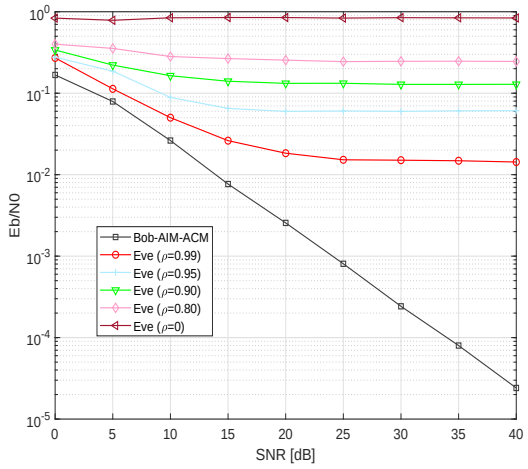
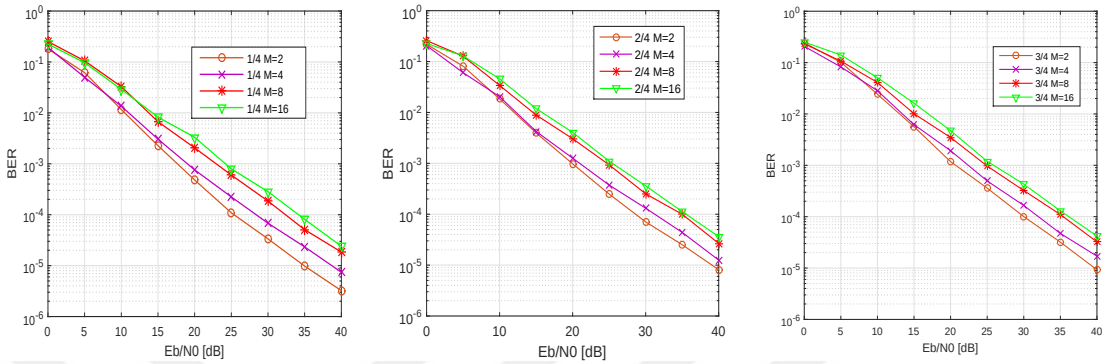


Fig. 6.18: BER comparison of Bob (OFDM-AIM-ACM) and Eve with correlation coefficient ($\rho = 0, 0.80, 0.90, 0.95, 0.99$).

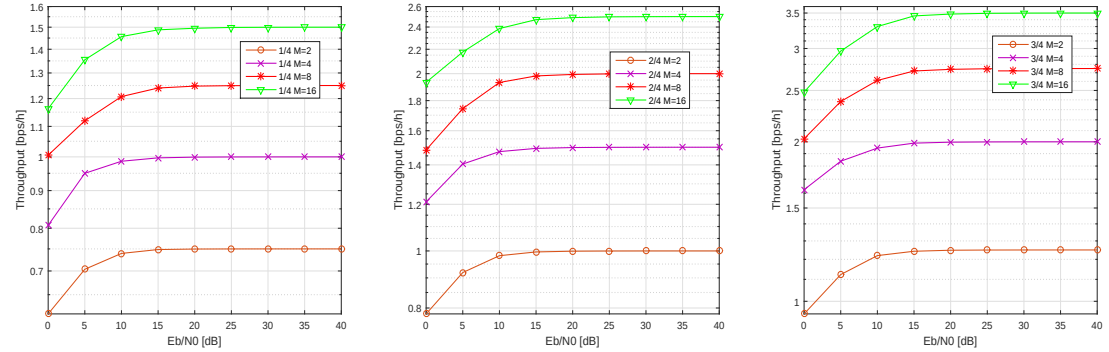
selected curves in the former step, we select those curves that have a performance gap among them. Finally, the resultant curves are presented in Fig. 6.20. c. Afterwards, the corresponding throughput curves of Fig. 6.20. e related to selected BER curves in Fig. 6.20. c are also selected and presented in Fig. 6.20. f.

Based on Fig. 6.20. c and Fig. 6.20. f, we develop a switching tables for QoS based communication in order to maximize the throughput. In this work, as an example, switching tables for the case of $BER < 10^{-3}$ and $BER < 10^{-4}$ are presented in Fig. 6.21[2]. The tables depict different SAR and CM values of system for different SNR ranges to maximize the spectral efficiency while fulfilling QoS requirements. Afterwards, these table can be used for QoS based communication for maximizing spectral efficiency in a similar way as performed in [124]. The result of OFDM-VIM-VCM for the case of $BER < 10^{-3}$ is presented in Fig. 6.20. f.

[2]Note: For the first row in Fig. 6.21.a and Fig. 6.21.b the range of values are from 0 to 19.9 and from 0 to 28.6, respectively.



(a) BER vs SNR (SAR=1/4).(b) BER vs SNR (SAR=2/4).(c) BER vs SNR (SAR=3/4).

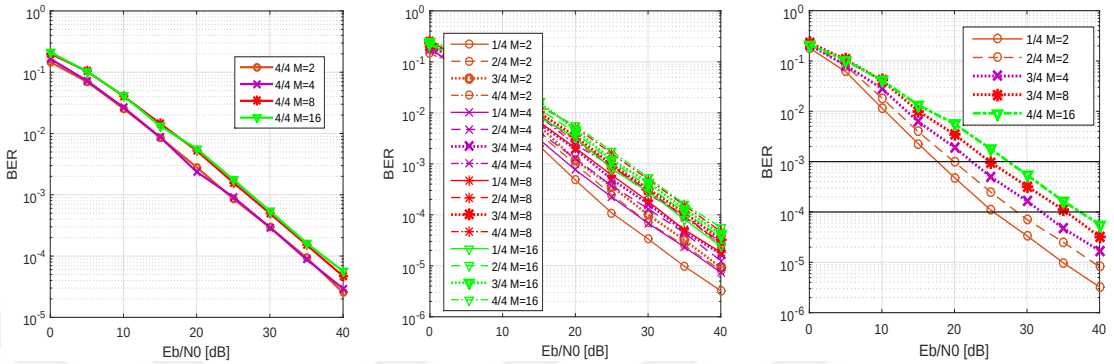


(d) Throughput vs SNR (SAR=1/4).(e) Throughput vs SNR (SAR=2/4).(f) Throughput vs SNR (SAR=3/4).

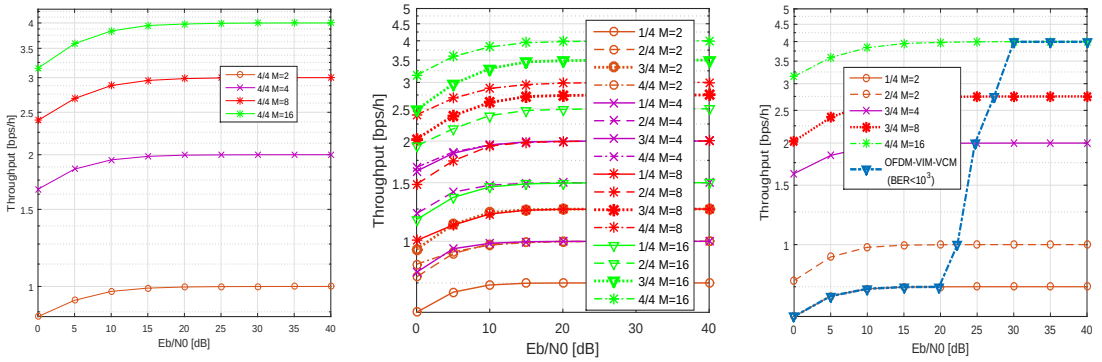
Fig. 6.19: OFDM-IM with SAR values of (1/4, 2/4, 3/4) and CM orders of (2, 4, 8 and 16).

6.6 Conclusion

In this work, effective algorithms that change SAR and/or CM adaptively in each subblock of the OFDM-IM scheme based on the channel characteristics of the legitimate receiver are proposed for enhancing PLS and SE. Particularly, the first two algorithms named as OFDM-AIM-FCM and OFDM-AIM-ACM are designed for enhancing PLS and SE, while the third algorithm named as OFDM-VIM-VCM is designed for QoS based communication for enhancing SE. Simulation results show that the first two algorithms can provide significant security enhancement



(a) BER vs SNR (SAR=4/4). (b) BER vs SNR (Merged). (c) BER vs SNR (Selective).



(d) Throughput vs SNR (SAR=4/4). (e) Throughput vs SNR (Merged). (f) Throughput vs SNR (Selective).

Fig. 6.20: OFDM-IM with SAR value of (4/4) and CM orders of (2, $M = 4$, $M = 8$ and $M = 16$), merged curves for different cases of OFDM-IM and selected curves for different cases of OFDM-IM for QoS based communication.

whereas the third algorithm ensures QoS based communication aiming to maximize spectral efficiency.

Eb/N0 (E)	BER < 10^{-3} M	SAR
17.6<E<19.9	2	1/4
19.9<E<22.4	2	2/4
22.4<E<24.8	4	3/4
24.8<E<27.4	8	3/4
27.4<E	16	4/4

(a) $BER < 10^{-3}$

Eb/N0 (E)	BER < 10^{-4} M	SAR
25.3<E<28.6	2	1/4
28.6<E<32	2	2/4
32<E<35.3	4	3/4
35.3<E<37.3	8	3/4
37.3<E	16	4/4

(b) $BER < 10^{-4}$

Fig. 6.21: Switching table for OFDM-VIM-VCM.

Chapter 7

Secure and Reliable IoT Communications Using Nonorthogonal Signals' Superposition with Dual-Transmission

7.1 Introduction

Fifth-generation (5G) wireless systems are not just simple evolution of conventional fourth-generation (4G) networks, but they are also expected to offer many new services beyond internet to critical communication and internet of things (IoT). The three main services of 5G include ultra-reliable low latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine type communication (mMTC) [8]. Overall, 5G will have a significant impact in many areas of life and will bring a lot of interesting applications such as autonomous driving, virtual reality, smart city, smart energy networks, remote surgery, drone

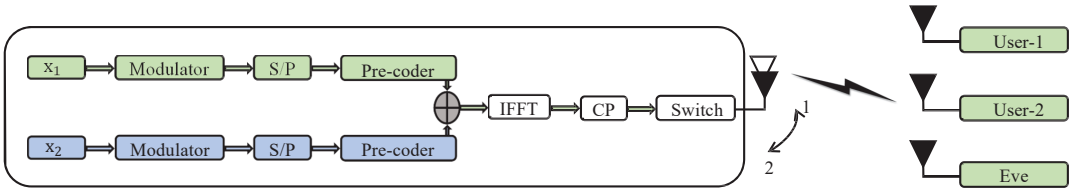


Fig. 7.1: Basic block diagram of pre-coder based multi-carrier IoT communication system with a single radio frequency chain and a single active antenna.

delivery, and so on. However, due to the broadcast nature of wireless communication, 5G is vulnerable to eavesdropping and intervention [145] [11], which may compromise the confidentiality of the signals.

The solutions to tackle security issues in wireless communication include cryptography and physical layer security (PLS) solutions [146]. Cryptography-based solutions are not suitable enough for future communication systems, especially for IoT-based applications. This is due to the fact that the heterogeneous nature of future communication makes the key sharing and management processes very challenging. Moreover, transceivers in some applications are processing restrict ed and power limited, making encryption-based algorithms unsuitable for them [10].

To solve the issues related to encryption-based solutions for future communication systems, PLS techniques have emerged as an effective solution that can complement the cryptography-based approaches [10]. PLS techniques can exploit the characteristics of wireless communication such as randomness, fading, noise, and interference to prevent unauthorized and illegitimate node to intercept or decode the legitimate communication. PLS techniques can exploit random channel between the legitimate parties to extract secret keys, thus, alleviating the need for key sharing. Moreover, various PLS techniques can be implemented by simple signal processing techniques and can support devices with limited processing and delay constraints such as IoT devices [11].

Among many top research areas in PLS, securing the orthogonal frequency division multiplexing (OFDM) waveform has got much attention. This is due to the fact that OFDM is not only one of the most popular and commonly used

waveforms in the current wireless communication system but it is also expected to be part of future communication with a wide variety of different numerologies [11]. The techniques proposed in the literature for PLS in OFDM can be grouped into four main classes. The first class is based on secret key generation algorithms in which the random wireless communication channel is exploited to generate secret keys [137]. The second class is related to channel adaptation assisted techniques in which the basic idea is to adapt the transmission parameters of the legitimate transmitter to enhance the performance of the legitimate receiver, for example, adaptive modulation and automatic repeat request based schemes [23], channel shortening [147], OFDM with sub-carrier index selection [148], etc. The third class is based on artificial noise-based techniques. In these techniques, the artificial noise is added based on the channel of the legitimate nodes in such a way that it can degrade the performance of eavesdropper without affecting the performance of the legitimate receiver [149]. The fourth class is based on algorithms that are based on concealing features of the OFDM waveform [98].

The aforementioned algorithms are effective security techniques but some of them were introduced without considering the unique requirements of 5G services. Moreover, there will be applications in the 5G and beyond networks that will require reliable and secure communication with processing limited receivers [148]. However, reliability and security conflict with each other [150]. This is because when the communication link quality is made very reliable, security is usually reduced because reliability comes with a lot of redundancy, which can increase the probability of eavesdropper in decoding the received data successfully [151]. Moreover, some of the security algorithms require complex processing at both transmitter and receiver which makes them infeasible for applications with a simple receiver. Based on the aforementioned discussion, in this work, we propose a simple dual-transmission based technique with a single active antenna transmitter for providing secure and reliable IoT communication systems. More specifically, data of IoT devices are superimposed using channel-based pre-coder matrices and sent in two transmissions to achieve reliable and secure communication against internal and external eavesdroppers.

7.2 System Model Assumptions

The considered system model consists of a multi-carrier downlink legitimate transmitter (Tx) with a single active antenna that is trying to communicate with two single-antenna legitimate IoT devices (users) in the presence of a passive single antenna external eavesdropper (Eve) as shown in Fig. 7.1. More specifically, the transmitter is equipped with two antennas and a single radio-frequency chain, where one of the antenna (antenna 1 or antenna 2) is made active for any transmission with the help of switch to artificially increase the randomness of the wireless channel for security enhancement. Furthermore, the users are assumed to be untrusted (internal eavesdropper), which means that the individual user's data is also needed to be secured from each other. It is also assumed that the transmitter has no knowledge about the channel of Eve. The channel between Tx and any user is assumed to be slowly varying multi-path Rayleigh fading with exponentially decaying power delay profile (PDP) and assumed to be known at the transmitter. Moreover, channel reciprocity property is also adopted, where the channel from the transmitter to the receiver and vice versa can be estimated by channel sounding techniques in time division duplexing (TDD) systems [147]. The legitimate transmitter wants secure communication with the users such that neither the external eavesdropper gets the information of the users' signals nor the users get each other's information.

7.3 Proposed Algorithm for Reliable and Secure Communication

The basic goal of this work is to fulfill the needs of those future applications that require reliable and secure communication and have limited processing capability at the receiver [148]. In this work, we superpose the signal of two users along with pre-coder matrices and sent the resultant signal in two transmissions while alternating the active antenna in each round. Having two transmission rounds, with each being transmitted from a different active antenna, is necessary to ensure

different channels during different transmissions. This, in turn, enables us to design and find a special type of pre-coders that can provide security against internal and external eavesdroppers simultaneously. Moreover, compared to the single-user channel-based security algorithm, two users with two transmissions introduce more difficulties to an eavesdropper. The reason is that in each round of the proposed algorithm the used pre-coders are function of different legitimate users' channels. However, in the case of single-user based algorithms, the pre-coder is a function of a single user's channel only. So, the two rounds job is to make it more difficult for an eavesdropper to decode the legitimate user's signal while making it easy for the legitimate users to decode the intended data. Moreover, the proposed algorithm just requires a single radio frequency chain at the transmitter.

The details of the proposed algorithm are as follows: As explained earlier, we consider a two-user single antenna multi-carrier system as presented in Fig. 7.1.

At the Tx, the total number of modulated symbols in one OFDM block for each user is N_f. Thus, the frequency response of each OFDM symbol for user-1 and user-2 can be represented as $\mathbf{x_1} = [x_0\ x_1\ .....\ x_{N_f-1}] \in \mathbb{C}^{[N_f \times 1]}$, and $\mathbf{x_2} = [x_0\ x_1\ .....\ x_{N_f-1}] \in \mathbb{C}^{[N_f \times 1]}$, respectively. Note that $\mathbf{y_{km}} \in \mathbb{C}^{[N_f \times 1]}$, $\mathbf{H_{km}} \in \mathbb{C}^{[N_f \times N_f]}$, and $\mathbf{z_{km}} \in \mathbb{C}^{[N_f \times 1]}$, respectively, represent the received signal, the diagonal matrix for frequency response of the channel, and additive white Gaussian noise (AWGN) between k_{th} user and m_{th} active antenna of the transmitter.

The basic idea is to first multiply each user signal with a specially designed channel-dependent pre-coder matrix. Afterwards, superimpose the pre-coded signals and finally send the resultant signal in two transmissions (rounds) in such a way that when the signals are combined at the legitimate receivers (IoT devices), each user will get its reliable signal by simply demodulating the combined signal without any complex processing. On the other hand, it will be very hard for eavesdroppers to detect the information intended for user-1 and user-2 due to legitimate users' channel-based specially designed pre-coder matrices. Moreover, the specially designed pre-coders will also make sure that the information of the

users is also secure from each other.

The basic steps for the design of pre-coder matrices for the proposed algorithm are presented in the subsequent discussion. On the basis of the proposed algorithm, the superimposed pre-coded transmitted signal during first round from active antenna-1 is given as:

$$\mathbf{u_1} = \mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}. \tag{7.1}$$

Similarly, the transmitted signal during the second round that is transmitted from active antenna-2 can be given as:

$$\mathbf{u_2} = \mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}, \tag{7.2}$$

where $\mathbf{x_1}$ and $\mathbf{x_2}$ are data vectors in frequency domain intended for user-1 and user-2, respectively, with equal power allocated to them, while $\mathbf{M_{1a}}$, $\mathbf{M_{2a}}$, $\mathbf{M_{1b}}$ and $\mathbf{M_{2b}}$ are specially designed pre-coder matrices based on the channel of legitimate nodes. These pre-coders will make sure that the user-1 and user-2 will get reliable signals which are also secure from internal and external eavesdropping. We will first explain the details about the received signal at user-1, user-2, and eavesdropper in the following two subsections. Afterward, the details about designing the pre-coding matrices will be explained.

7.3.0.1 Received Signal at User-1

The received signal in the frequency domain at user-1 during round-1 using active antenna-1 can be given as:

$$\mathbf{y_{11}} = \mathbf{H_{11}u_1} + \mathbf{z_{11}}, \tag{7.3}$$

where $\mathbf{H_{11}}$ and $\mathbf{z_{11}}$ are the frequency response of the channel and AWGN noise between user-1 and active antenna-1 of the Tx during round-1. Similarly, the received signal at user-1 during round-2 using active antenna-2 is given as:

$$\mathbf{y_{12}} = \mathbf{H_{12}u_2} + \mathbf{z_{12}}, \tag{7.4}$$

where $\mathbf{H_{12}}$ and $\mathbf{z_{12}}$ are the frequency response of the channel and AWGN between user-1 and active antenna-2 of the Tx during round-2. The combined received signal from round-1 and round-2 at user-1 can be written as:

$$\mathbf{\hat{y}_1} = \mathbf{y_{11}} + \mathbf{y_{12}}, \tag{7.5}$$

where $\mathbf{y_{11}}$ and $\mathbf{y_{12}}$ are the received signals at user-1 during round-1 and round-2 through active antenna-1 and active antenna-2, respectively. After putting the values of $\mathbf{y_{11}}$ and $\mathbf{y_{12}}$, the combined signal can be given as follows:

$$\mathbf{\hat{y}_1} = \mathbf{H_{11}u_1} + \mathbf{z_{11}} + \mathbf{H_{12}u_2} + \mathbf{z_{12}}. \tag{7.6}$$

Substituting the values of $\mathbf{u_1}$ and $\mathbf{u_2}$ from (7.1) and (7.2) and simplifying, we get:

$$\begin{aligned}\mathbf{\hat{y}_1} = \mathbf{H_{11}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{11}} \\ + \mathbf{H_{12}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{12}},\end{aligned} \tag{7.7}$$

$$\begin{aligned}\mathbf{\hat{y}_1} = (\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}})\mathbf{x_1} + (\mathbf{H_{11}M_{2a}} \\ + \mathbf{H_{12}M_{2b}})\mathbf{x_2} + \mathbf{z_{11}} + \mathbf{z_{12}}.\end{aligned} \tag{7.8}$$

The first term in (7.8) is the desired term with respect to user-1 while the second term is undesired term. The pre-coder matrices will make sure that the undesired term as well as the channel effects are removed and canceled at user-1.

7.3.0.2 Received Signal at User-2

Similar to user-1, the combined received signal from round-1 and round-2 for the case of user-2 can be written as:

$$\mathbf{\hat{y}_2} = \mathbf{y_{21}} + \mathbf{y_{22}}, \tag{7.9}$$

where $\mathbf{y_{21}} = \mathbf{H_{21}u_1} + \mathbf{z_{21}}$ and $\mathbf{y_{22}} = \mathbf{H_{22}u_2} + \mathbf{z_{22}}$ are the received signals at user-2 during round-1 and round-2 through active antenna-1 and antenna-2, respectively. $\mathbf{H_{21}}$ and $\mathbf{z_{21}}$ are the frequency response of the channel and AWGN between user-2 and active antenna-1 of the Tx during round-1 while $\mathbf{H_{22}}$ and $\mathbf{z_{22}}$ are the frequency response of the channel and AWGN between user-2 and active antenna-2 of the Tx during round-2. After putting the values of $\mathbf{y_{21}}$ and $\mathbf{y_{22}}$, the combined signal can be presented as:

$$\hat{\mathbf{y}}_\mathbf{2} = \mathbf{H_{21}u_1} + \mathbf{z_{21}} + \mathbf{H_{22}u_2} + \mathbf{z_{22}}. \tag{7.10}$$

Substituting the values of $\mathbf{u_1}$ and $\mathbf{u_2}$ from (7.1) and (7.2) and simplifying, we get:

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{2} = \mathbf{H_{21}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{21}} \\ + \mathbf{H_{22}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{22}}.\end{aligned} \tag{7.11}$$

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{2} = (\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}})\mathbf{x_1} + (\mathbf{H_{21}M_{2a}} \\ + \mathbf{H_{22}M_{2b}})\mathbf{x_2} + \mathbf{z_{21}} + \mathbf{z_{22}}.\end{aligned} \tag{7.12}$$

The first term in equation (7.12) is the undesired term for user-2 while the second term is desired term for it.

7.3.0.3 Received Signal at Eavesdropper

For the case of eavesdropper, the combined received signal from round-1 and round-2 can be written as:

$$\hat{\mathbf{y}}_\mathbf{3} = \mathbf{y_{31}} + \mathbf{y_{32}}, \tag{7.13}$$

where $\mathbf{y_{31}} = \mathbf{H_{31}u_1} + \mathbf{z_{31}}$ and $\mathbf{y_{32}} = \mathbf{H_{32}u_2} + \mathbf{z_{32}}$ are the received signal at eavesdropper during round-1 and round-2 through active antenna-1 and antenna-2,

respectively. $\mathbf{H_{31}}$ and $\mathbf{z_{31}}$ are the frequency response of the channel and AWGN between eavesdropper and active antenna-1 of the Tx during round-1 while $\mathbf{H_{32}}$ and $\mathbf{z_{32}}$ are the frequency response of the channel and AWGN between eavesdropper and active antenna-2 of the Tx during round-2. After putting the value of $\mathbf{y_{31}}$ and $\mathbf{y_{32}}$, the combined signal can be presented as:

$$\hat{\mathbf{y}}_{\mathbf{3}} = \mathbf{H_{31}u_1} + \mathbf{z_{31}} + \mathbf{H_{32}u_2} + \mathbf{z_{32}}. \tag{7.14}$$

Substituting values of $\mathbf{u_1}$ and $\mathbf{u_2}$ from (7.1) and (7.2) and simplifying as follows:

$$\begin{aligned}\hat{\mathbf{y}}_{\mathbf{3}} = \mathbf{H_{31}}(\mathbf{M_{1a}x_1} + \mathbf{M_{2a}x_2}) + \mathbf{z_{31}} \\ + \mathbf{H_{32}}(\mathbf{M_{1b}x_1} + \mathbf{M_{2b}x_2}) + \mathbf{z_{32}},\end{aligned} \tag{7.15}$$

$$\begin{aligned}\hat{\mathbf{y}}_{\mathbf{3}} = (\mathbf{H_{31}M_{1a}} + \mathbf{H_{32}M_{1b}})\mathbf{x_1} + (\mathbf{H_{31}M_{2a}} \\ + \mathbf{H_{32}M_{2b}})\mathbf{x_2} + \mathbf{z_{31}} + \mathbf{z_{32}}.\end{aligned} \tag{7.16}$$

The eavesdropper wants to get information about both user-1 and user-2. Hence, for it, both the first and second terms of (7.16) are desired terms.

7.3.0.4 Pre-coder Design for the Proposed Algorithm

We need to design pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{2a}}$, $\mathbf{M_{1b}}$ and $\mathbf{M_{2b}}$ in such a way that the combined signal during round-1 and round-2 at the legitimate users will provide reliable data intended for them while keeping the communication secure from internal and external eavesdropping.

The design procedure of $\mathbf{M_{1a}}$ and $\mathbf{M_{1b}}$ is as follows: Firstly, in order to remove the effect of channel at user-1, the first term in the equation (7.8) should be equal to identity matrix and can be given as:

$$(\mathbf{H_{11}M_{1a}} + \mathbf{H_{12}M_{1b}}) = \mathbf{I}. \tag{7.17}$$

Also, in order to cancel the interference caused by user-1 on user-2, the first term in equation (7.12) should be zero and can be given as:

$$(\mathbf{H_{21}M_{1a}} + \mathbf{H_{22}M_{1b}}) = 0. \tag{7.18}$$

Equations (7.17) and (7.18) can be jointly solved to get the values of pre-coder matrices $\mathbf{M_{1a}}$ and $\mathbf{M_{1b}}$ as follows:

$$\mathbf{M_{1a}} = \mathbf{H_{22}}(\mathbf{H_{22}H_{11}} - \mathbf{H_{21}H_{12}})^{-1}. \tag{7.19}$$

$$\mathbf{M_{1b}} = -\mathbf{H_{21}}(\mathbf{H_{22}H_{11}} - \mathbf{H_{21}H_{12}})^{-1}. \tag{7.20}$$

Similarly, in order to design $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$, we will follow similar steps as explained earlier. In order to remove the effect of the channel at user-2, the second term in equation (7.12) should be equal to identity and can be given as:

$$(\mathbf{H_{21}M_{2a}} + \mathbf{H_{22}M_{2b}}) = \mathbf{I}. \tag{7.21}$$

Also, in order to cancel the interference caused by user-2 on user-1, the second term should be zero in equation (7.8) and can be given as:

$$(\mathbf{H_{11}M_{2a}} + \mathbf{H_{12}M_{2b}}) = 0. \tag{7.22}$$

Equations (7.21) and (7.22) can be jointly solved to get the values of pre-coder matrices as follows:

$$\mathbf{M_{2a}} = \mathbf{H_{12}}(\mathbf{H_{12}H_{21}} - \mathbf{H_{11}H_{22}})^{-1}. \tag{7.23}$$

$$\mathbf{M_{2b}} = -\mathbf{H_{11}}(\mathbf{H_{12}H_{21}} - \mathbf{H_{11}H_{22}})^{-1}. \tag{7.24}$$

The values of pre-coder matrices $\mathbf{M_{1a}}$, $\mathbf{M_{1b}}$, $\mathbf{M_{2a}}$ and $\mathbf{M_{2b}}$ are given in equations (7.19), (7.20), (7.23) and (7.24), respectively, will be used in round-1 and round-2 to make sure that the user-1 and user-2 will get reliable signals which are secure from internal and external eavesdroppers. Note that, in the proposed method explained earlier, we do not need any complex processing at the receiver of user-1 and user-2 and they just simply need to add the signals from round-1 and round-2. Hence, it can support applications with processing limited receiver (IoT-based applications).

7.4 Simulation Results

In this section, simulation results for the proposed algorithm are presented in order to evaluate the effectiveness of the proposed technique by using bit error rate (BER), throughput, and peak to average power ratio (PAPR) as performance metrics.

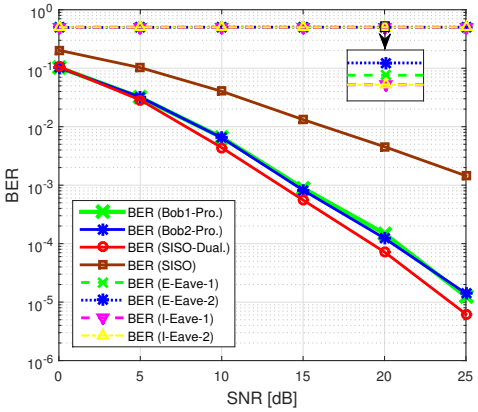


Fig. 7.2: BER versus SNR performance for the proposed algorithm, SISO with dual-transmission, and SISO-OFDM.

We consider that the Tx is employing OFDM with $N_f = 64$ sub-carriers with BPSK modulation for each user and a cyclic prefix (CP) of size L is added in order to avoid inter-symbol interference (ISI). The channel is assumed to be multi-path Rayleigh fading channel between the transmitter and receiving nodes (such as users and eavesdropper) with an equal number of taps ($L = 9$).

Fig. 7.2 shows the BER versus signal to noise ratio (SNR) plots for the proposed algorithm, single-input single-output (SISO)-OFDM system, and SISO with the dual-transmission (SISO Dual.), where SISO with dual-transmission is used as a benchmark. Note that in SISO with dual-transmission, the OFDM symbol is transmitted two times to have a fair comparison with the proposed algorithm. It should be noted from Fig. 7.2 that the BER performances of user-1 (Bob1-Pro.) and user-2 (Bob2-Pro.) employing the proposed algorithm are similar to each other. However, there is a significant gap between their BER performances and that of external eavesdropper ones, where labels E-Eve-1 and

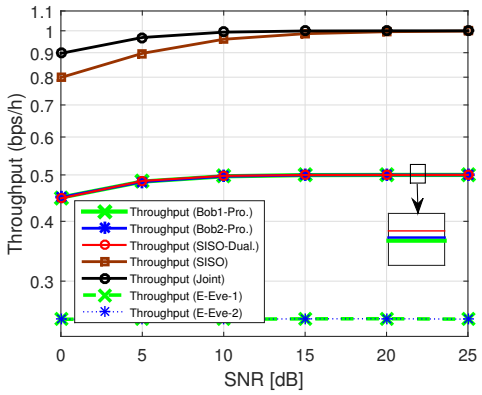


Fig. 7.3: Throughput versus SNR performance for the proposed algorithm, SISO with dual-transmission, and SISO-OFDM.

E-Eve-2 present the BER performances of the external eavesdropper that is trying to eavesdrop the signals intended for user-1 and user-2, respectively. Fig. 7.2 also shows that there is a significant gain in BER performances of users employing the proposed algorithm and SISO with dual-transmission (SISO Dual.) as compared to SISO-OFDM performance. Moreover, it is also observed that there is a little performance degradation of users employing the proposed algorithm compared to SISO with the dual-transmission (SISO Dual.). However, SISO with the dual-transmission cannot provide secure communication while the proposed algorithm can provide significant gain in terms of security against internal and external eavesdropper.

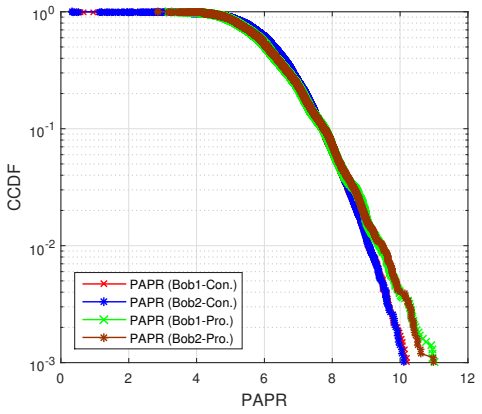


Fig. 7.4: Comparison of PAPR performances of the conventional OFDM and proposed algorithm.

Fig. 7.4 presents the throughput versus SNR plots for the proposed algorithm, SISO-OFDM system, SISO with the dual-transmission (SISO Dual.), and joint consideration of users throughput. The reason for the joint consideration of throughput is that the superimposed signals of user-1 and user-2 are sent jointly during each transmission in the proposed algorithm such that the total number of packets sent by the proposed algorithm is similar to the case of SISO. It is observed

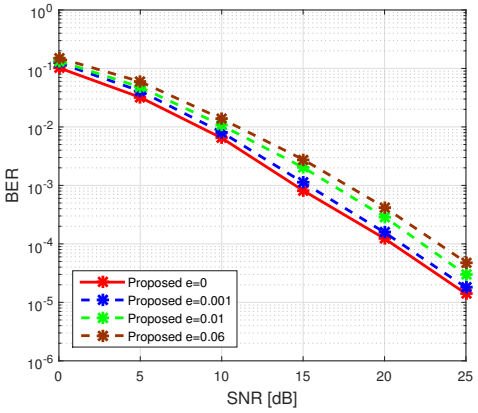


Fig. 7.5: BER versus SNR performance of the proposed algorithm for imperfect case.

from Fig. 7.3 that the individual throughput performances of user-1 (Bob1), user-2 (Bob2), and SISO with the dual-transmission are similar to each other while worst compared to SISO-OFDM case and joint case. It is also observed from Fig. 7.3 that the throughput performance of the joint case outperforms SISO-OFDM at lower values of SNR while it has similar performance to the joint case at high SNR. Moreover, it is observed that the performances of throughput for external eavesdroppers are worse. One important point to be noted here is that although the throughput performances of the external eavesdroppers are not zero, quality of service (QoS) based security can still be ensured. Here, the QoS based security [23] means to provide security based on the requirements of different services (voice, video, etc.) instead of providing perfect security. More specifically, different services have different QoS requirements for reliable communication and if we make sure that eavesdropper is operating below the QoS requirements of a specific service, we can secure that service.

Fig. 7.4 depicts a comparison of the peak to average power ratio (PAPR)

performances of the conventional OFDM and OFDM with the proposed algorithm for user-1 (Bob1) and user-2 (Bob2). It is observed from Fig. 7.4 that there is a small degradation in the PAPR performances of the users compared to conventional OFDM. Overall, the proposed algorithm can be a good solution for providing secure communication, especially for IoT devices with limited processing receivers.

Analyzing the robustness of the PLS algorithm against the imperfect channel is extremely important. In order to show the effect of the imperfect channel, intentional error ($\Delta\mathbf{h}$) is added to the true channel ($\mathbf{h}$). The imperfect channel is given by $\tilde{\mathbf{h}} = \mathbf{h} + \Delta\mathbf{h}$ [147]. We can model $\Delta\mathbf{h}$ as an independent AWGN with zero mean and variance ($\sigma^2 = e \times 10^{\frac{-SNR_{dB}}{10}}$), where the value of e determines the quality of estimator, with lower values showing a good quality estimator. Fig. 7.5 shows the BER versus SNR performance under imperfect channel conditions with estimators having different qualities ($e = 0, 0.001, 0.01, 0.06$). It is observed from Fig. 7.5 that there is a small degradation in the BER performance of the proposed algorithm due to the imperfect estimator. However, it can be improved by increasing the power of training sequence or/and by using a pilot with a longer length. Moreover, there are plenty of algorithms in the literature to enhance the channel estimator's performances [147].

7.5 Conclusion

An effective technique for reliable and secure communication is presented for IoT devices. Channel-dependent pre-coders with dual-transmission approach are jointly exploited to ensure a reliable as well as secure communication against internal and external eavesdropping. More specifically, users' pre-coded data is superimposed in the first step. Afterward, the mixture is sent in two transmissions in such a way that after combining signals from the first and the second transmissions, the legitimate receivers will get the reliable signal without complex processing while the external eavesdropper will get the degraded version of the signal. Moreover, the proposed algorithm also ensures that the users are also

not able to eavesdropper each other's data. Simulation results proved that the proposed algorithm can ensure secure communication and suitable for IoT-based devices because it does not require complex processing at the receivers. For future work, the extension of the proposed algorithm for active eavesdropper case will be considered.

Chapter 8

Secure Communication via Untrusted Switchable Decode-and-Forward Relay

8.1 Introduction

Due to the advantages of wireless communication over wired communication, wireless-based applications are becoming extremely pervasive in our daily life. Furthermore, with the advancement in high data-rate-based applications, the demand for bandwidth and power efficient transceivers is continuously increasing [152]. To this end, cooperative communication is a suitable candidate for providing bandwidth efficient transceivers, especially for handheld devices. More precisely, amplify-and-forward (AAF) and decode-and-forward (DAF) are the most popular techniques of cooperative communications [153]. In [154], the authors presented hybrid relaying scheme for Orthogonal Frequency Division Multiplexing (OFDM) system, which takes benefits of both DAF and AAF relaying by adaptively switching among AAF, DAF and non-relay modes on subcarrier basis. Although AAF and DAF are popularly used schemes in the literature, they have some problems related to noise enhancement and error propagation. These

problems can be overcome by using efficient channel coding schemes [153], [155] such as convolutional encoding with Viterbi decoding [156], [157].

In addition, the security aspect of wireless communication is one of the most critical issues due to the broadcast nature of wireless communication [158]. The use of wireless communication for sharing sensitive information (e.g. financial transactions, personal information, etc.) makes security one of the most critical requirements for the current and future wireless systems [158]. Conventional techniques for security have mainly focused on cryptography but the key's establishment and management are very complex tasks in modern decentralized networks [159]. In order to solve this issue, the research on physical layer security (PLS) has drawn a lot of interest because of its ability to solve the challenges offered by the conventional cryptographic-based security techniques. The PLS techniques are capable of providing confidentiality by utilizing the impairments of wireless channel, such as noise, fading, interference, etc. [158], [159].

This study concerns about PLS techniques for cooperative communication systems. There is a variety of such PLS techniques [159], such as PLS-based secret key generation using relays [160], relay-based beamforming for PLS with and without cooperative jamming [161], relay selection for enhancing PLS [162], adaptive power allocation dependent PLS techniques [163], noise and cooperative jamming dependent PLS techniques with trusted and untrusted relay [164], [14], etc.

In this study, we mainly focus on cooperative jamming with untrusted relay. In [164], an untrusted relay was jammed with the help of an external node or the intended receiver in such a way that it helps in the reliability but cannot extract information from the signal. In [14], a technique composed of two phases was proposed to provide secrecy. In its first phase, the source transmits a signal towards relay, and simultaneously cooperates with the destination for jamming the eavesdropper. In its second phase, the decoded source signal is transmitted by the relay, and at the same time, this relay cooperates with the source to jam the eavesdropper.

In the case of untrusted AAF relay, destination-assisted jamming is an effective technique, which takes advantages of relay, while keeping information secure from the relay. However, in the case of untrusted DAF relay, the destination-assisted-jamming based security techniques do not work because jamming signals from destination affect the performance of DAF relaying [165]. Hence, DAF relaying had not been used in untrusted network as discussed in [15]. Although AAF's implementation is simple, it may amplify the noise [153], so coded DAF [156] is preferable. Motivated by [154] and destination-assisted jamming for AAF [165], a practical technique for secure communication via DAF untrusted relay is proposed. This technique allows the users to keep utilizing the benefits provided by DAF, while keeping the information secure from the untrusted relay.

8.2 System Model and Preliminaries

The system model, presented in Fig. 8.1, consists of a source, a destination, and a relay in a two-hop half-duplex relay-aided system. In this system, an untrusted switchable DAF (sDAF) relaying based cooperative communication is considered. Its normal/actual operation is DAF but it can be switched to AAF relaying in certain predefined switching conditions because of simplicity of AAF relaying.

The relay is assumed to be passive and it can only store one frame at a time, which means that it must forward the current frame in order to get a new frame. It is also assumed that each node can either transmit or receive a signal at a given time slot. In Fig. 8.1, the notations h_{sd}, h_{sr} and h_{rd} denote Rayleigh fading coefficients from source to destination, source to relay and relay to destination, respectively. All of these coefficients are modeled as zero mean complex Gaussian random variables [153].

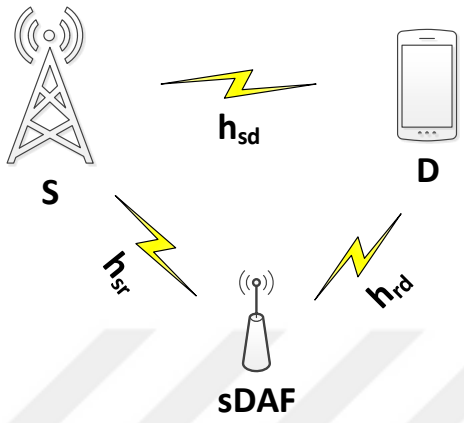


Fig. 8.1: Basic system model for cooperative communication system.

8.3 Proposed Method

In this section, the proposed algorithm is explained. The algorithm is based on TDMA protocol and it is divided into two phases.

(A) Phase 1: In the first phase, the source shares RMS with destination through untrusted sDAF relay in the presence of interference signal from destination.

(B) Phase 2: In the second phase, the shared RMS is used for establishing secure cooperative communication through untrusted sDAF.

The process of phase switching is explained at the end of this section. For reliability improvement and efficiency, coded cooperative communication system is considered in this protocol. The explanation details of two phases of this algorithm are as follows:

8.3.1 Phase 1

In this phase, our system is in AAF mode. In the first time slot, T0, of phase 1, the source encodes RMS [157], modulates it and sends a frame X_{RMS} of QPSK modulated signal, while at the same time the destination transmits the jamming signal X_j [165] as presented in Fig. 8.2. It is assumed that the destination can either transmit or receive signal at a given time slot, so in T0, it is only transmitting interference signal. The received signal at the relay in the time slot T0 is given by

$$Y_{r1} = h_{sr}X_{RMS} + h_{rd}X_j + n_{sr}, \tag{8.1}$$

where Y_{r1} is the received signal and n_{sr} represents additive white gaussian noise (AWGN) with the variance σ^2 at source to relay link. The Signal to inteference ratio (SINR) at relay is given by

$$SINR_{p1}^{R} = \frac{|h_{sr}|^2}{\sigma^2 + |h_{rd}|^2} \tag{8.2}$$

where $|h_{rd}|^2$ is the interference due to the jamming signal from destination.

The mutual information M_{p1}^{R} at relay in phase 1 is given by

$$M_{p1}^{R} = \frac{1}{2}\log_2\left(1 + \frac{|h_{sr}|^2}{\sigma^2 + |h_{rd}|^2}\right), \tag{8.3}$$

where we assume the transmission power at the destination and the source to be the same. In the second time slot, T1, the relay amplifies the mixed signal and forwards it to the destination. The transmitted signal at T1 is given by

$$X_{r1} = \frac{Y_{r1}}{amp}, \tag{8.4}$$

$$amp = \sqrt{|h_{sr}|^2 + |h_{rd}|^2 + \sigma^2}, \tag{8.5}$$

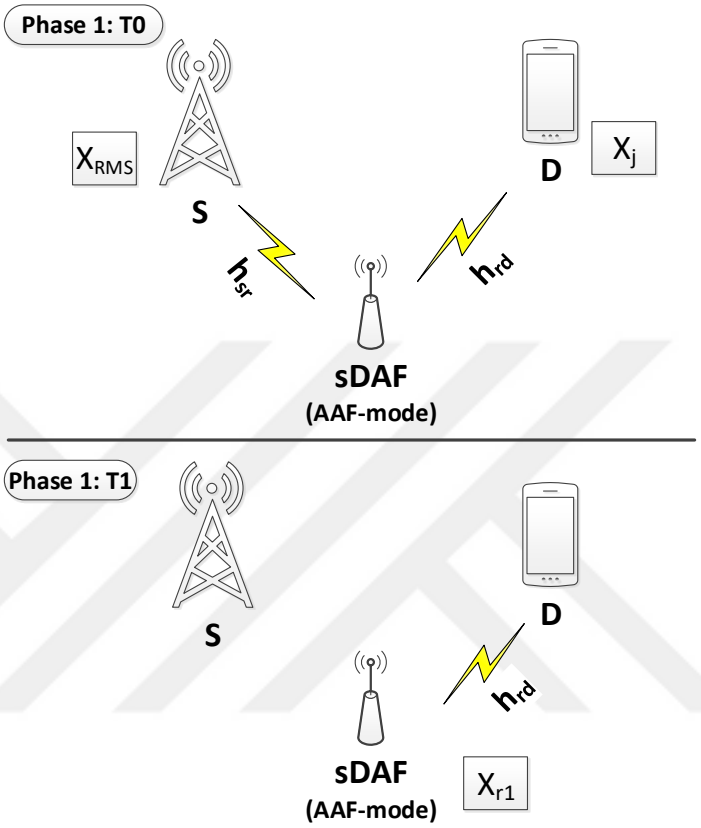


Fig. 8.2: Phase 1 (RMS sharing)

where amp is the normalization coefficient for power. It should be mentioned that due to the jamming signal from the destination, the untrusted relay cannot decode it successfully, even if it tries. In the time slot T1, the received signal at destination from relay is given by

$$Y_{1d} = \frac{1}{amp} h_{rd} h_{sr} X_{RMS} + \frac{1}{amp} h_{rd}^2 X_j + \frac{1}{amp} h_{rd} n_{sr} + n_{rd}, \tag{8.6}$$

where Y_{1d} is the received signal at the destination and n_{rd} is the AWGN at the relay to destination link.

The SINR at destination

$$SINR_{p1}^{D} = \frac{\frac{1}{amp^2}|h_{sr}|^2|h_{rd}|^2}{\frac{1}{amp^2}|h_{rd}|^2\sigma^2 + \sigma^2} \tag{8.7}$$

Since X_j was generated by destination, such jamming signal will not degrade the performance at destination. The mutual information M_{p1}^{D} at destination in phase 1 is given by

$$M_{p1}^{D} = \frac{1}{2}\log_2\left(1 + \frac{\frac{1}{amp^2}|h_{sr}|^2|h_{rd}|^2}{\frac{1}{amp^2}|h_{rd}|^2\sigma^2 + \sigma^2}\right), \tag{8.8}$$

The destination can remove the interference from received signal because it knows the interference signal that it has sent in the time slot T0. So, at the end of phase 1, the destination demodulates and decodes the RMS.

The achievable secrecy rate with sDAF in phase 1 for is given by

$$\begin{aligned} SR = \frac{1}{2}\log_2\left(1 + \frac{\frac{1}{amp^2}|h_{sr}|^2|h_{rd}|^2}{\frac{1}{amp^2}|h_{rd}|^2\sigma^2 + \sigma^2}\right) \\ - \frac{1}{2}\log_2\left(1 + \frac{|h_{sr}|^2}{\sigma^2 + |h_{rd}|^2}\right). \end{aligned} \tag{8.9}$$

It should be noted that at high SNR the factor $\frac{|h_{sr}|^2}{\sigma^2+|h_{rd}|^2}$ in M_{p1}^{R} is constant and the value of M_{p1}^{R} is negligible which ensure that RMS can not be intercepted at sDAF. The reason of negligible value of M_{p1}^{R} at relay is due to fact that interference from destination degrades the performance of signal at relay.

8.3.2 Phase 2

In the second phase of our algorithm, the cooperative system switches back to its normal (DAF) operation. In this phase, the source uses the RMS (from phase 1) for data manipulation, and then encodes it, modulates it, and finally transmits

a frame of secure symbols X_s in the first time slot, T0, of phase 2, that will be received by relay and destination as presented in Fig. 8.3. The received signals at relay and destination in time slot T0 are given by

$$Y_{r2} = h_{sr}X_s + n_{sr}, \tag{8.10}$$

$$Y_{d2_1} = h_{sd}X_s + n_{sd}, \tag{8.11}$$

where Y_{r2} and Y_{d2_1} are the signals received at relay and destination, respectively, while, n_{sd} is AWGN at source to destination link. In the second time slot, T1, the relay will decode and then re-encode the data, modulate it, and then forward it to the destination. The received signal at destination in time slot T1 is given by

$$Y_{d2_2} = h_{rd}X_r + n_{rd}, \tag{8.12}$$

where Y_{d2_2} is the received signal at destination in slot T1. The destination will use the signals from T0 and T1 for final decoding. After decoding, the receiver will extract information by using RMS signal.

One of the important factors in this algorithm is the relay mode switching. In the literature, switching is controlled by SNR based algorithm [157], but in this work, a simple case for switching, which is referred to as hard switching, is considered. In hard switching, the system goes through phase 1 at the start of the communication (once or for a certain predefined number to minimize errors), and then it switches back to normal phase 2. In our system, the RMS can be updated by switching back to phase 1 from phase 2 after a certain predefined number of frames, which completely depends on the required security level, complexity and delay. The relay mode switching can also be done by sending a feedback from destination to relay and source.

In comparison to the conventional cooperative jamming techniques introduced

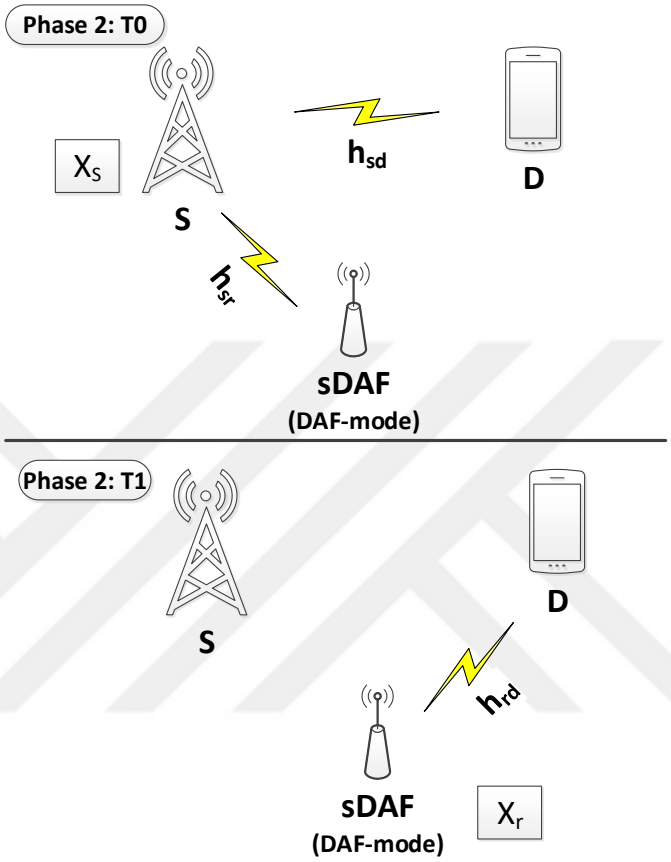


Fig. 8.3: Phase 2 (Secure DAF)

in the literature [13-15], in which continuous jamming signal is required to be sent from source, helping relay or destination, the proposed algorithm does not require continuous jamming signal. Instead, it requires jamming signal only during phase 1 of the algorithm for sharing RMS. So, this fact makes the proposed algorithm more power efficient as compared to others jamming based security schemes.

It should be mentioned that the proposed algorithm can also be applied in the scenarios where there is no direct path between source and destination.

8.4 Simulation Results

In this section, simulation results are presented by using bit error rate (BER) as a metric to analyze the effectiveness of our proposed security method [166]. In this study, the effects of imperfect channel estimation, that may occur due to interference, synchronization and noise errors are taken into account by adding intentional independent estimation errors at the destination and the relay. These estimations errors are based on values of mean square error (MSE) of a least square estimator (LSE) [166], [167].

The estimated erroneous channels at destination can be modeled as $\hat{h}_{sd} = h_{sd} + \Delta h_{sd}$, where h_{sd} is the perfect channel and Δh_{sd} is modeled as independent complex Gaussian noise vector with zero mean and error variance $\sigma^2 = e \times 10^{\frac{-SNR_{dB}}{10}}$, where, $e = 0.2$ is considered here. It should be noted that the value of error variance can be improved by using estimators of good quality. For the case

Table 8.1: Simulation parameters

No. of bits per frames	1000
Modulation	BPSK
Channel encoding	1/2 Convolution Codes
Channel Decoder	Viterbi Decoder
Code rate	1/2
Memory	2
Channel	Rayleigh fading channel

of h_{sr} and h_{rd}, similar assumptions for imperfect channel estimation are made as described above. The basic parameters for both encoder and decoder for phase 1 and phase 2 are presented in Table 8.1.

In phase 1, sDAF is in AAF-mode with destination-assisted interference to secure RMS from untrusted relay as explained in Section III. The BER performance of AAF-mode (phase 1) for both perfect channel estimation (PCE) and imperfect channel estimation (IPCE) is presented in Fig. 8.4 by abbreviation "sDAF-P1(PCE)" and "sDAF-P1(IPCE)", respectively. It is observed that IPCE leads

to a small degradation in BER that can be overcome by using training sequence of larger length and higher power.

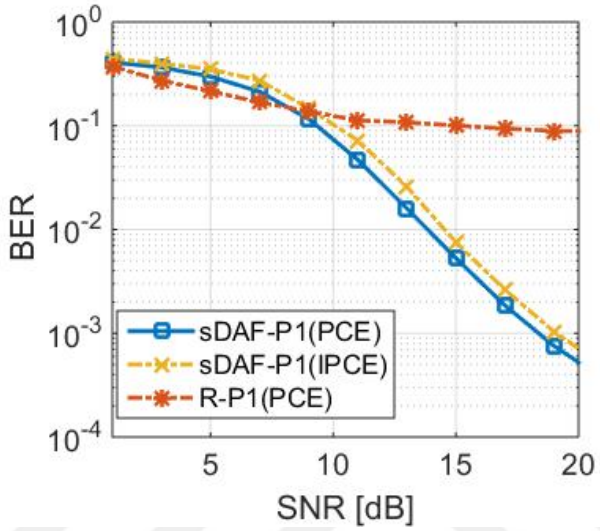


Fig. 8.4: BER performance for phase 1.

As explained in section III, phase 1 is used to transmit RMS that will be used in phase 2 for secure communication. It should be noted that errors in RMS are minimized to a negligible value by sending multiple interleaved copies of RMS frames in phase 1 at high SNR, and by comparing different copies. The significance of interference from destination in phase 1 is that even if relay tries to decode the signal, it cannot decode it properly, as presented by abbreviation "R-P1(PCE)" in Fig. 8.4. This is due to fact that at approximately high SNR values the value of M_{p1}^{R} is negligible which ensure that RMS can not be intercepted at sDAF. The securely transmitted RMS will be used in phase 2 for manipulating data. Fig. 8.5 presents results for phase 2. In the first time slot of phase 2, the relay and the destination receive RMS-manip ulated encoded data from the source. The relay first decodes the received data by using the Viterbi decoder and then re-encodes the data, modulates it and transmits it to the destination in the next slot. The destination uses symbols from time slot 1 and time slot 2 to apply Viterbi decoder after demodulation. After decoding the data, the destination will extract information from decoded data by using RMS as explained in Section III. The performance of RMS-manipulated DAF versus average SNR for PCE and IPCE

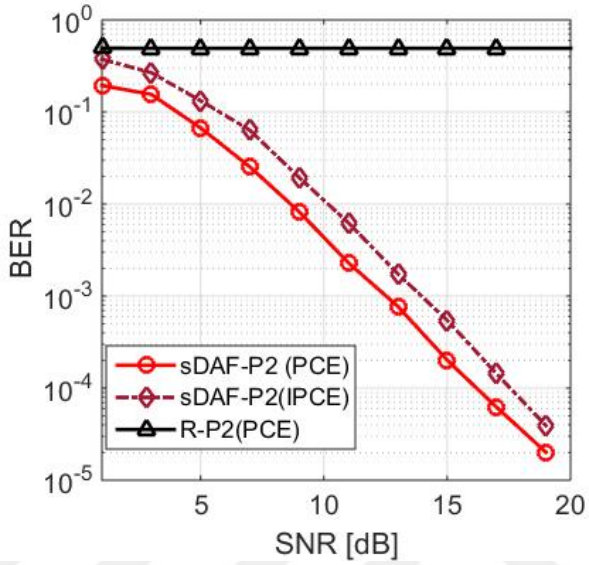


Fig. 8.5: BER performance for phase 2.

of our algorithm is presented in Fig. 8.5 by abbreviation "sDAF-P2(PCE)" and "sDAF-P2(IPCE)", respectively. The performance of RMS-manipulated DAF is better than AAF relaying in the presence of effective channel coding scheme as presented in Fig. 8.5. The BER versus SNR performance at relay in phase 2 is presented by abbreviation "R-P2(PCE)". Due to RMS manipulation the relay is not able to decode the data properly. Hence, this algorithm provides secure communication in the presence of untrusted DAF relay.

8.5 Practical Insights on the Proposed Scheme

It is important to mention that unlike many of the existing physical layer security techniques, whose design is channel-dependent, making them extremely prone and vulnerable to channel reciprocity mismatch and estimation errors, our proposed security technique is channel-independent. This merit helps ease and facilitate the practical implementation of the proposed security technique, making it hardware-friendly.

8.6 Conclusion

In this work, a reliable and power efficient security technique for an untrusted DAF based cooperative communication is proposed. The technique enables us to keep utilizing the benefits provided by DAF relay, while keeping information secure from it. The proposed technique is more power efficient as it does not require continuous power for jamming signal. The simulation results are provided to demonstrate the effectiveness of the proposed algorithm for both perfect and imperfect channel estimation cases. Future studies can examine untrusted-relay-assisted D2D based heterogeneous networks and untrusted secondary users in cognitive communication.

Chapter 9

Cognitive Security of Wireless Communication Systems in the Physical Layer

9.1 Introduction

The proliferation of wireless technologies in our daily life leads to an increasing demand for these technologies. While the prevalence of wireless communication systems presents indisputable advantages to the users, due to the open broadcast nature of the wireless signals, the communication exchanges are exposed to the attacks of adversaries. As opposed to its wired counterparts, the enhanced mobility support of the wireless communication systems comes with the handicap of serious security vulnerabilities from the physical layer to the application layer. To protect the wireless signals from malicious attacks, security measures should be provided to the user. In the existing wireless communication systems, security concerns are addressed in the upper layers by means of various encryption techniques. Encryption is achieved in such a way that the message is encrypted with a key generated by using cipher, i.e., an encryption algorithm, before the signal is transmitted. The receiver can decrypt the message by using the same

key. However, since encryption is a way of protecting the message in the upper layers, it does not prevent the signal from being detected by adversaries in the medium. Additionally, encryption increases the infrastructural overhead and power consumption to enable the authentication, which may not be feasible in some applications such as wireless sensor networks [168]. Data security in wireless domain has to adapt itself to the new wireless communications paradigm by becoming more adaptive and flexible. To this end, implementation of communication security in the physical layer has recently become a field of interest. Existing security threats in the physical layer can be categorized into three groups: Eavesdropping, jamming, and spoofing as depicted in Fig.9.1. In the physical layer security studies, legitimate transmitter, legitimate receiver and passive attacker are symbolized, respectively, as Alice, Bob, and Eve. The attacker might be considered as either a jammer or a spoofer if attacker is active.

1. *Eavesdropping:* When Alice transmits a message to Bob, any receiver can receive the message since the message is propagated through the whole environment. Eavesdropping refers to a situation where Eve can receive the message transmitted by Alice. The message needs to be protected against the eavesdroppers.

2. *Jamming:* When Alice and Bob are communicating with each other, a jammer transmits a noise type of signal to Bob with the aim of corrupting the communication. When Bob receives both signals at the same time, legitimate signal would be received as meaningless signal. Therefore, the signal would not be decoded. This type of attack is named as jamming. When the attack is held, it needs to be identified by legitimate users, and the signal needs to be protected accordingly.

3. *Spoofing:* Spoofing refers to a situation where the attacker deceives Bob. Spoofing can be carried out in two ways: a) When Alice stops transmitting the signal, an attacker starts to transmit a deceiving signal to Bob. b) When Alice transmits the signal, if an attacker transmits deceiving signal with higher power than Alice's signal power, Bob would receive the attacker's signal as legitimate signal while it would consider Alice's signal

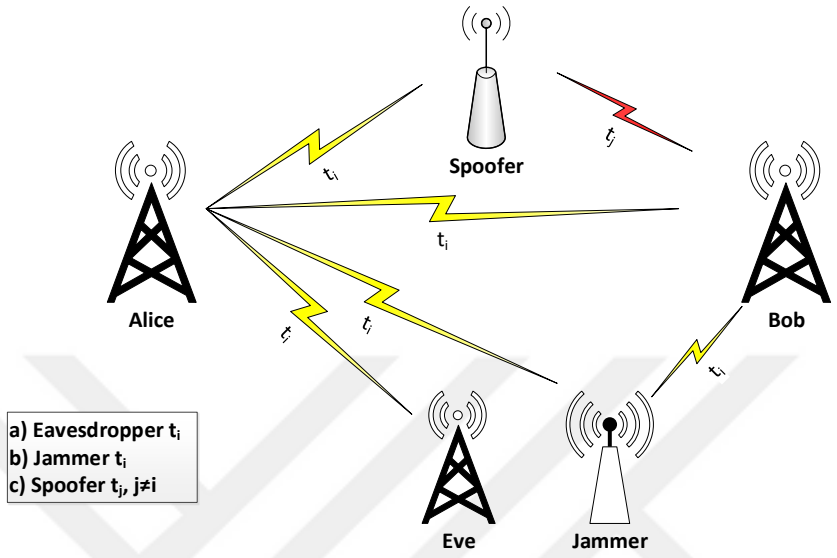


Fig. 9.1: When Alice transmits a message to Bob at time t_i, a) Eavesdropper receives/listens the same message at time t_i, b) Jammer transmits a jamming signal to Bob at time t_i, c) Spoofer listens the message at time t_i and then transmits a spoofing message at time t_j where $t_j \neq t_i$.

as interference signal. Similar to the jamming case, this attack needs to be identified and necessary precautions should be taken.

In the literature, studies on physical layer security mainly focus on spread spectrum (SS) techniques, channel and power based solutions. In SS techniques, the energy of the signal is spread over the wider spectrum by means of possessing a wider band. SS techniques are particularly useful against the jamming attacks and eavesdropping. In eavesdropping case, these techniques are used to attain the low probability of interception and detection. Frequency hoping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are primary SS techniques used in the literature. FHSS is derived by hopping the signal with a predefined pseudo-random code in the spectrum while in DSSS the energy of the signal is spread over a wide spectrum with a pseudo noise (PN) sequence which keeps the signal power under noise level. As mentioned in [169], these techniques can be utilized to provide security against jamming attacks with certain vulnerabilities. For instance, FHSS technique may be vulnerable against spoofing attacks . To overcome this issue, an anti-jamming scheme that is based

on transmitting a secure identity generated with cryptographic methods is proposed in [170]. Thus, the legitimate transceiver communication can be protected against jamming and spoofing attacks. The drawbacks of DSSS scheme against jammers are investigated in [171]. This drawback is defined in such a way that when :PN sequence of jammer is matched with the transmitter's :PN sequence, the legitimate receiver can be jammed. To address this drawback, authors propose a watermarked DSSS scheme. In this scheme, an authentication information is embedded to :PN sequence to make the system more resistant against jamming attacks.

In channel based solutions, the uniqueness feature of the channel can be utilized to improve security. Since the communication channel between Alice and Bob is different from the channel between Eve and Bob, Alice can perform a secure communication by using its unique channel with Bob. The effects of artificial noise insertion in the presence of Eve is explored in [172]. The primary objective of the artificial noise insertion is to degrade Eve's channel while not affecting Bob's channel. To carry out this aim, Alice adds noise intentionally to the null spaces of Bob's channel. Since, Eve does not know the intentional addition of noise, she is not able to detect the signal correctly. Thus, the secure communication would be satisfied even if Eve's channel is not known. Primarily, eavesdropping and spoofing can be prevented with channel based solutions.

In power based solutions, received signal strength (RSS) and directional antenna are used to provide security. RSS is utilized to detect the primary user (PU) emulation attack in [173]. In the cognitive radio network, there are PUs and secondary users (SUs). SUs use the licensed spectrum of PUs. If PU utilizes any bands in its spectrum, SU does not use the same band in order not to cause interference on PU. To determine which bands are utilized by PU, SU can use spectrum sensing algorithm. There might be spoofers in the environment to deceive SUs by masquerading the PU. A verification algorithm to detect the spoofers is proposed in [173] by utilizing the signal characteristics and location of the legitimate transmitter. RSS measurements are performed within a wireless sensor network. All transmitters locations can be estimated by identifying the RSS peaks. In [174], directional antennas are explored against jamming attacks

instead of the more conventional omni-directional antennas. The connectivity is maintained under jamming attacks with directional antennas. Since there are multiple antennas in Bob, certain antennas can easily be reconfigured towards a direction other than the direction where the jamming signal is coming from. In this case, the transmitter can keep the connectivity with the legitimate receiver with higher data rate when compared to omni-directional antenna usage case. Wyner introduces the wiretap channels, namely eavesdropper's channel in [175]. He aims at rendering the signal meaningless taken by wire-tapper. To achieve this, Wyner utilizes signal-to-noise ratio (SNR) differences observed at Bob and Eve. If Eve's SNR is lower than Bob's SNR, Alice can initiate a secret communication with Bob without any information leakage to Eve via encoding.

While the aforementioned studies provide a security only in the physical layer, the security in cross layer is investigated in the following studies. The requirements and benefits of cross layer security are presented for wireless sensor network (WSN) in [176]. As explained in [176], cross layer design should work collaboratively to detect the adversaries while enabling the efficient power consumption. The cross layer utilization by means of the intrusion detection is proposed in [177]. It is proved that security which is obtained by exploiting the data coming from different layers such as link and network layers is increased significantly when compared the single layered security solutions in terms of true positive rates.

Besides the studies focusing on the specific security issue, in a few studies, the physical layer security literature is surveyed. In each of these papers, authors examine the security studies from different perspectives. In [178] and [179], and from a bigger picture in [180] and [181], authors investigate the security in cognitive networks. While authors in [182] explain the security issues in health care domain, authors in [183] look at these issues in smart grid applications.

9.2 Motivation

Although existing efforts satisfy the security needs of the users under certain conditions and for specific wireless communications systems, they might fail in others. For instance, since channel based solutions have complete dependency on channel conditions, while these solutions would work when legitimate transceiver is static and has reciprocal channel, these solutions would fail when the legitimate transceiver is either mobile or performs communication based on frequency division duplexing. Alternatively, SS techniques can be employed to protect data against jamming attacks and eavesdropping. When there is a spoofer in the environment, if an additional protection algorithm as given in [170] is not proposed, SS technique would fail. Moreover, using an additional algorithm would increase the complexity of the legitimate transceiver. Another issue with SS techniques is related to :PN or hopping sequence sharing. When a legitimate transmitter sends :PN or a hopping sequence to a legitimate receiver, if the sequence is not protected, an illegitimate node can capture this secret information. Therefore, illegitimate node can easily eavesdrop, jam, or spoof the legitimate receiver. As explained in Section 9.1, power based solutions would help to locate the users against spoofing and jamming attacks. In RSS based localization, it is assumed that illegitimate node uses omni-directional antennas and multiple receivers measure the RSS of this node to be able to perform true localization. If illegitimate node employs the directional antenna, localization would fail [184]. Power based solutions therefore would not provide security against eavesdropper since the location of eavesdropper is unknown.

All of these weaknesses of the existing solutions indicate the necessity that the security threats need to be investigated with more comprehensive solutions in the physical layer. In this study, we propose cognitive security (CS) concept which provides adaptive security solutions in the communication systems by exploiting the physical layer security from different perspective. The adaptiveness relies on the fact that radio adapts its propagation characteristics to satisfy secure communication based on specific conditions. In this paper, the conditions are defined as the user density, application specific adaptation, and location. Please note

that, in the existing efforts, security is provided when the legitimate transceiver is under attack(s). However, the security is performed in CS concept before the attack occurs. In other words, CS proposes that the necessary precautions are required to be taken before the attack takes place based on the conditions which are explained in detail in the subsequent sections. Thus, the systems would adjust the propagation parameters of the radio against possible threats. With the given conditions, CS should:

- Increase the reliability in the wireless communication systems. Since transceiver would be able to adjust the security level, increasing the security adaptively will increase the overall reliability of the communication system automatically. Especially, when a receiver is under jamming attack, one of the most important problems is to satisfy reliable communication to guarantee the quality of service requirement. CS would play an important role in this situation.

- Decrease the system complexity. The active attackers need to be detected in current security mechanisms. This requires additional algorithms to be implemented in the systems. Since, in CS concept, detecting the attackers is not necessitated, this would reduce the complexity caused by the usage of the additional algorithms.

  Along with these advantages, CS should also:

- Increase the data rate. The radio resources allocated for providing secure communication can be reduced for the cases which do not necessitate high level of security due to low probability of threat. For instance, if the security is based on the location, let say, in rural areas, security level is lowered when compared to urban areas. Since some resources which are allocated to provide security would remain empty, these resources will be used for data communication. Thus, the users who live in rural areas would have higher data rates.

- Decrease the energy consumption. It is important to lower the consumed energy in the systems during the communication, e.g., in mobile devices.

If security level is lowered in uplink, the mobile device would be able to transmit the same amount of data in less duration since the data rate would be higher.

9.3 Cognitive Security Concepts

The system model for cognitive physical-layer security is illustrated in Fig.9.2. The radio combines the relevant information obtained from the radio channel and environment. Based on the available knowledge, the context is detected. To improve the detection performance, the statement information can be attained from the upper layers. After an associated security mechanism is determined by the radio, the level of the security can be adjusted as a function of the intensity of threat.

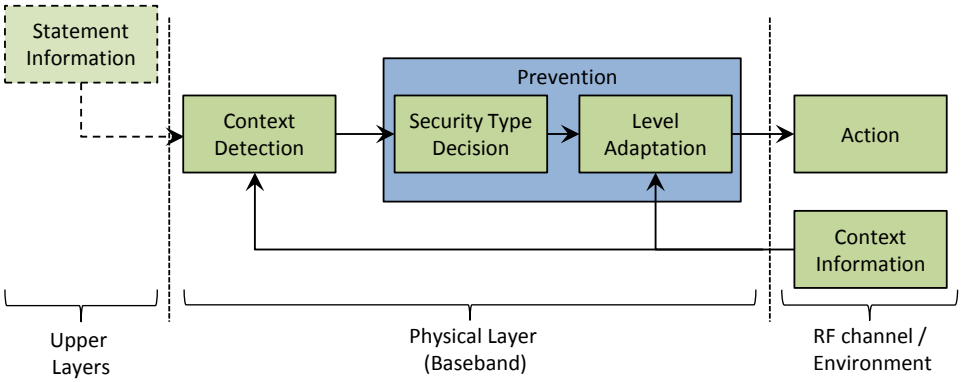


Fig. 9.2: System model for cognitive security

In this study, we define three the CS concepts: User density, application specific adaptation and location.

9.3.1 User Density

User density refers to a number of users per unit area. If the number of users is high in a given area when compared to a predetermined normal, e.g., schools,

hospitals, it can be stated that the area has high density in terms of the number of users and named as high user density through the rest of the paper. From the security perspective, high user density is an important parameter, especially for CS concept. As mentioned in Section 9.1, there are three threat groups in physical layer security studies. The radio can act intelligently to provide secure communication in spite of the fact that these three groups are probable to occur related to the user density. For specific places such as hospitals, office blocks, airports, security is highly important. Jammers, eavesdroppers or spoofers are expected to exist in such places as shown in Fig.9.3. In [185], authors define the probability of eavesdropping (or attacking) in a given area A.

$$P(e) = 1 - e^{-\rho A} \tag{9.1}$$

where ρ is the node density. For a given area, when the node density increases, probability of eavesdropping increases as well.

Density is the detectable data by the radio. In a high user dense area, since most of the resources would be occupied by the users, the detection of the density can be achieved by observing the total number of allocated resources at a time. When high density is detected, attackers would aim to affect the communication in between legitimate users, for instance, between a patient and a doctor in the hospital. Implantable medical devices (IMDs) such as defibrillators and peacemakers are implanted within the patient's body and are monitored and controlled by the physician with the help of external unit wirelessly. This wireless nature will make the IMDs vulnerable to attacks which might disrupt the communication by jamming or sending wrong information to the legitimate receiver by spoofing. In both cases, if the patient is in a critical condition and needs an emergent treatment, since the doctor won't be able to know the patient's situation because of jamming or spoofing, s/he will not treat his/her patient. The result might therefore be fatal for the patient. In this case, to immune to attacks, the radio might increase the security. If the high user density stems from the office block, legitimate users might be eavesdropped. The aim of the eavesdropper is to capture the company's critical information. Another important issue is that there might be many jammers, eavesdroppers, or spoofers who work collaboratively in high user dense areas. The security can possibly be improved significantly by

adaptively adjusting the propagation parameters of the radio.

There might be various reasons for users to gather in a given area such as stadium, hospital, school, or airport. Since it is not possible for a radio to detect the reason of users' gathering, the necessary information can be obtained from the upper layers. For instance, if the users in the high dense area send important documents, this can be detected by the upper layers and this information is provided to radio. Based on this notice, radio can consider that the density stems from the employees who work in an office block. This type of security approach is named as cross layer security in the literature [176]. As defined in Section 9.2, one of the key advantages of CS is to increase the data rate. If a holistic approach is not considered, data rate might be decreased unnecessarily in some cases. For instance, assume that the security should be higher in office blocks than the security in stadiums. Since radio does not have the reason of users' gathering, it would increase the security to the same level in all high user dense areas. This may not be desirable for every situations. For the same amount of user data, high secure communication might necessitate more resources to be allocated than less secure communication. Therefore, data rate in the relevant dense area would decrease. When the density in question is occurred in the stadiums, data rate would become more critical. The security level in the stadium should not be the same as the one in the office blocks. This situation can be considered as the probability of error in the increment level of security.

9.3.2 Application Specific Adaptation

Application specific refers to different fields such as military, commercial, and health monitoring in which the radio is used. Communication is typically held wirelessly in these fields. To minimize or alleviate the interference, different frequency bands are allocated for each field. These different bands carry significant context information for the radio. This helps the radio to detect the type of application for which the communication is being fulfilled.

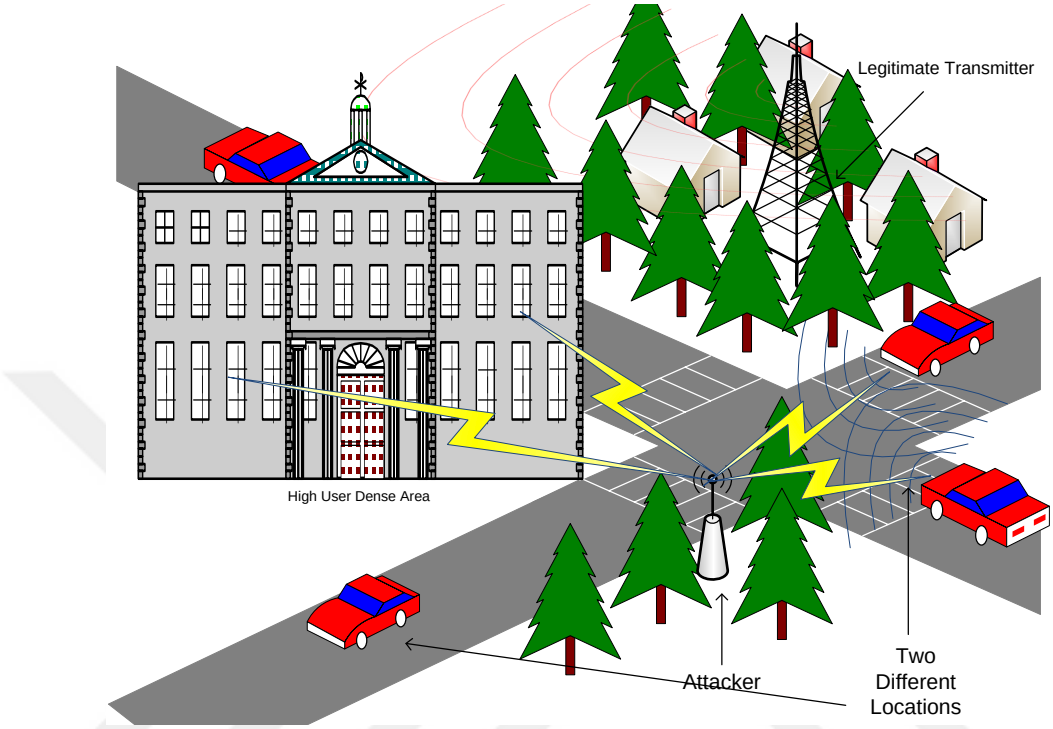


Fig. 9.3: Attackers would appear in the user dense areas. Also, they are more likely to jam or spoof the vehicular communication in the intersections.

Each application has different security requirement. While it is high for military communication, it might be low for commercial applications, such as for cellular communication. Ensuring secure communication requires more resources to be allocated and a higher data rate is vital for commercial sector. Allocating as many resources as in military communication for security reasons to carry out the communication may therefore not be feasible in commercial domain. In any case, communication needs to be provided securely when the transceiver is under attacks. Existing security threats would differ based on time and place where the communication is being held for each application. For instance, when the country is in peace, passive attacks like eavesdropping would be significant for military communication. But, if there is an emergency situation such as a battle, jamming and spoofing are going to be very serious issues as well. In these types of situations, security needs to be adjusted accordingly. The existing algorithms which are proposed to protect the data from eavesdroppers may not provide the security in jamming or spoofing scenarios as mentioned in Section 9.2. This indicates that securing the communication against each type of attacks necessitates

different solutions. In any emergency situation, military may need to reach out to the public across the country or may need additional resources for the communication. To meet this demand, military has to utilize certain ubiquitous structures such as cellular base stations and broadcasting antennas. Although security level might be lower in cellular communication when compared to military, when the emergency situations occur, radio should be able to detect it and adapt itself to new situations. Since the cellular or broadcasting structure is not suitable to implement the same security methods, the radio should provide more secure communication via the physical layer security mechanisms. Herein, military would protect its communication against jamming or spoofing attacks. If the security level depends on the application, it needs to be adaptively managed.

One another important application is the internet of things (IoT) for future wireless networks. Various types of technologies such as implantable medical devicess (IMDs), WSN, autonomous vehicles will share the bands in IoT. These different technologies may require different level of security. For instance, while it is critical to provide high security for IMD, it may need less security in smart home applications such as controlling the refrigerator over the internet. Therefore, CS will play an important role in 5G and beyond networks in terms of providing and adjusting necessary security and data rate needs for each application.

9.3.3 Location

Specific location or social environment where the communication is fulfilled is an important parameter for CS concept. For some devices such as unmanned aerial vehicles (UAVs), the location information is required to find their geographical position. Therefore, it is important to provide security against attacks based on the location information. It can be said that, there is a high correlation between the type of the security threats and the location. For instance, for vehicle-to-vehicle (V2V) communication, location determines the type of the communication between vehicles. When two vehicles go back-to-back on the road, the communication is performed to maintain a minimum distance between

vehicles, namely space cushion, through the sensors at all times to not cause an accident. Alternatively, when two vehicles encounter an intersection where there is a significant decision making process, the type of the communication would be different. One issue is the order of the vehicles to cross the intersection [186]. While this example highlights the importance of the location in terms of the type of the V2V communication, this location information is also critical to satisfy the secure communication between vehicles. The two vehicles at the intersection point need to talk to each other while simultaneously monitoring the measurement of the sensors to detect any possible rear vehicle. This may lead to some security gaps to attack the vehicles that are at the intersection point as depicted in Fig.9.3. In this situation, there are two possible security issues: Jamming and spoofing. An attacker may destroy the communication of the vehicles or may send the same message to two vehicles such as the priority of who would pass first. Both situations would eventually cause an accident. The security level can be significantly increase if the radio is able to detect the location. Thus, the accident may be precluded.

In terms of social environment, three types of environments can be considered: Rural, suburban and urban areas. The main difference between the environment types is the population density. At this point, it is important to emphasize that the social environment should not be confused with user density in terms of the detectability. As mentioned above, user density definition covers a small area such as stadiums, schools, and it can be within urban, suburban and rural areas. However, environment covers the whole urban, suburban, or rural area by definition.

In wireless communication, environment information is important in terms of the capacity. For instance, to increase the capacity, various deployment strategies of the base stations (BSs) are applied. While the BSs whose coverage area is as high as 1-2 km might be sufficient to serve for the users in rural areas, the small BSs whose coverage area is around 10-200 m would need to be deployed in urban areas to meet the users' demands. To provide a secure communication, environment is a significant parameter. Based on the environment type, security need would differ, especially in the public safety context. The crime rates are much

higher in urban areas. For example, 39 crimes are recorded per 1,000 residents in rural areas while 79 crimes are reported in urban areas in England. To decrease the crime rate, governments need to take necessary preventions. When a crime or an emergency situation occurs, each unit of the system, e.g., mobile devices, networks etc., should work coordinately and securely so that the relevant government agent can act promptly. If the system is under jamming or spoofing attacks, the communication might be disrupted. Therefore, a high security level should be provided for each unit. Since, most of the time, this is the case for the urban areas, radio should adaptively increase the security based on the environmental information for the wireless systems. In conclusion, the type of environment also determines the level of security rather than just the security itself.

Figure 9.4 shows the relation between security needs and type of environment in terms of probability of attacks. This figure is drawn, i.e. not based on simulation, to only help readers to visualize this relation. The probability of attack increases in the urban areas when compared to rural areas. It is also visualized that the increasing probability of attack increases the usage of resources for security reasons, which also leads to decreasing data rate.

Another importance of the location information is related to the devices which have dependency on accurate geographical position such as UAVs. While UAVs can be controlled from a ground station, they can also have pre-installed location and mission information and perform duty automatically. In both cases, UAVs necessitate location information obtained from global positioning system (GPS) satellites. Attackers would intend to disrupt the communication between UAV and GPS satellite.

Please note that UAVs are used for different purposes in different areas. While they are used for policing in public safety, they are also utilized in scientific researches, for disaster relief, and in armed attacks. Each type of usage may require the security in different levels in terms of localization. While the low level of security might be enough to provide communication in disastrous relief cases with the aim of obtaining high data rate, high level of security would be necessary in armed attacks. On the other hand, when the country is in battle, UAVs used

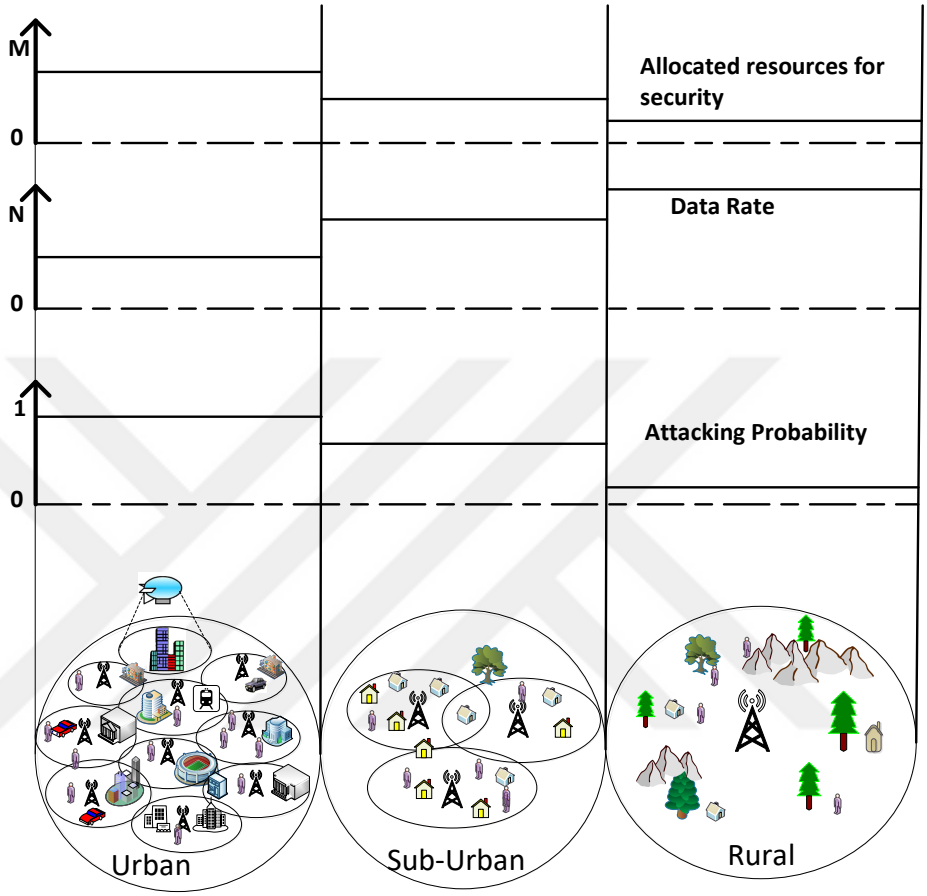


Fig. 9.4: Based on the environment information, security needs can change. While the probability of attack might be higher in urban areas, it might be low in rural areas. The increased probability of attack increases also the resource usage to provide higher security, which also leads to decreased data rate.

for other purposes such as for commercial usage can also be utilized to defend the country against the enemies. Since the enemies' aim would be to disrupt or spoof the communication between UAVs and GPS satellites, UAVs would need to increase the security accordingly to not be harmed or controlled by the enemies.

As highlighted above, the aim in this study is to take the necessary precautions based on some conditions, any type of new security mechanism is therefore not proposed within CS concept. Instead, three different conditions are given to help radio to determine if the security is a need or not. In Table 9.1, the benefits of the CS concept related to security threats are enlisted. After the security need occurs,

Table 9.1: Advantageous of Cognitive Security Concept against Security Threats

Security Threats	Explanation of Cognitive Security Conditions	Benefits
Eavesdropping	* Increase the secrecy rate (vs. information rate) in scenarios of high user dense areas such as office blocks, airports or locations such as urban areas or specific applications such as military, public safety * Relax the secrecy constraints, i.e., increase the information rate, for conditions such as rural areas, WiFi, cellular communication	Data rate, Latency, Energy Consumption
Jamming	* The level of security against jamming, e.g., processing gain in spread spectrum, is adaptively increased in locations such as intersections of roads, or specific applications such as military, public safety	Reliability, Complexity, Latency
Spoofing	* Enable the spoofing detection mechanism when the condition exists, and disable the algorithm, or use a simpler method, in high user dense areas such as office blocks, stadiums, or locations such as intersections of roads & location dependent UAV devices, or specific applications such as military, in-vivo communication	Complexity, Reliability

any current security solution can be utilized. At this point, it is worth mentioning that the CS should not be confused with context-aware security concept. In context-aware security, the information is mainly obtained by different sensors. Based on the these information, the system in upper layers tries to detect if there is an attack. If so, then, the necessary security algorithm is placed. In other word, the focus in context-aware security is on providing the necessary security when it is a need based on the context information such as temperature, speed etc. [187] as in conventional approaches in the security studies [180] and [181]. In CS, the security need is determined based on the conditions regardless of the attack occurs.

In Fig. 9.5, we compare the CS with fixed security (FS), in which the security level is the same for any conditions, for the user density case in terms of rate vs the number of eavesdropper. The rate is computed as $Rate = \sum_i \log_2(1+SNR_i)$. where i is the antenna index. As given in (9.1), when the user density increases in a given area, the probability of eavesdropping also increases. Based on (9.1), we realize this increment as the increasing number of eavesdropper in the figure. We assume that Alice transmits the signal to Bob from multiple antennas and there are multiple eavesdroppers working collaboratively. We assume that the transmitter utilizes multiple antennas with artificial noise to provide security during communication with Bob. Invoking that the signal transmitted by multiple antennas can be considered as multidimensional signal, one of these dimensions is allocated for the data transmission to Bob while the remaining ones are used for the artificial noise transmission. In FS case, we assume that the number of transmit antennas of Alice is fixed. In this case, when the number of eavesdroppers increases, Eve's rate will also increase. Since only fixed number of antennas is

used to send artificial noise signal, the desired security will be achieved only for the cases where the number of Eavesdroppers are less than the number of dimensions allocated for the artificial noise at the transmitter. Therefore, the sum rate of the eavesdroppers will increase by increasing the number of collaborating malicious nodes. For this case, the rate of Bob will remain constant. In CS case, the number of transmit dimensions for the artificial noise of Alice changes with the number of eavesdroppers in the environment. While the security level of eavesdropper stays the same because of having constant rate, Alice's rate decreases. It is because the total transmit power of Alice is fixed and shared between the data and artificial noise signals.

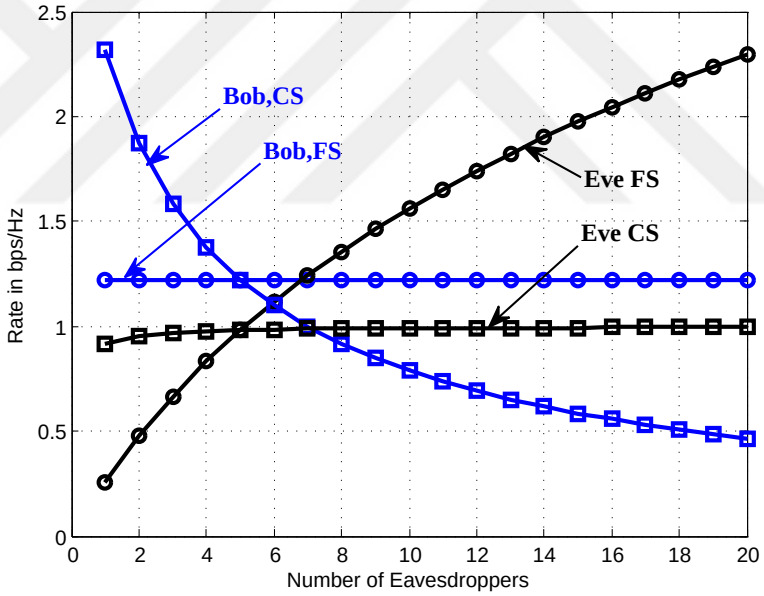


Fig. 9.5: When the number of eavesdropper increases in a given area, while the rate of Bob remains constant in the FS case, it is decreasing in CS. However, in terms of the security, CS provides higher security than FS case.

9.4 Conclusion & Open Issues

Providing security in wireless communication is a critical task. In this paper, we focused on the security in physical layer where we proposed CS concept. Radio can adapt its security level in CS by considering three different conditions which

are defined as user density, application specific adaptation, and location. These conditions come along with certain challenges which can be listed as:

9.4.1 How to detect if the condition exists?

To make the security adaptive, ensuring the detectability of context information is critical. While some of the context information such as user density is easy to detect via available spectrum sensing techniques [188], for some of them such as application specific, it is a hard task. As explained in Section 9.3.2, when the country is in battle and the military needs to use the cellular stations and frequencies for the communication, radio should have the capability to increase the security. Here, the question arises as to how the radio realizes that condition. If there is a need to obtain some parameters from the upper layers to detect the context information, how should radio collaborate with those layers? Collaboration between the layers is also a subject of cross-layer techniques [176].

9.4.2 How to identify the correct statement about the context?

As mentioned in Section 9.3.1, detailed knowledge might be needed to adapt the security level after detecting the existence of context information. For instance, the reason of users' gathering can be an entertainment event which might not necessitate a high security level while it can be required in business environments. How one can differentiate the statement of the context emerges as a hot topic.

9.4.3 What type of security mechanism can be used and how much resource should radio allocate?

There are many studies to secure the communication in physical layer most of which focus on specific circumstances. Especially, after detecting the context

information and identifying the correct statement, the third step is: 'Other than current efforts, what type of security mechanisms should be performed depending on the information captured from the environment and upper layers?'. Will this new method provide higher security than the existing efforts? For which context will it be a remedy? Regardless of whether a new method is proposed or any existing solution is used, how is the security level adjusted? For instance, based on the security threat, the waveform can be determined in the physical layer. If there is a jamming attack, spread spectrum waveform can be utilized. In this case, the security level can be considered as the processing gain, i.e., the amount of spreading. As a final note, the adaptation ability of a specific technique to change the security needs should also be considered. For instance, transmit power can be a limiting factor for some users which might restrict the flexibility of the security level in artificial noise insertion based techniques. Alternatively, in SS, total available bandwidth needs to be considered while performing the adaptation.

In this study, we provided different conditions which necessitate CS. However, it is highlighted that various new context information can be integrated into CS concept by taking the dynamic nature of the wireless communication systems.

Chapter 10

Physical Layer Security for Downlink NOMA: Requirements, Merits, Challenges, and Recommendations

10.1 Introduction

Non-orthogonal multiple access (NOMA) has received significant attention for 5G and beyond wireless systems due to its unique properties such as high spectral efficiency, low latency, improved coverage, massive connectivity, fairness and so on [189]. However, compared to orthogonal multiple access (OMA), there are some critical security risks in NOMA. More specifically, due to the broadcast of superimposed messages from multiple users at the same time over the same resources, there is a risk that an eavesdropper can overhear the information of multiple users if NOMA transmission is successfully intercepted. Moreover, in NOMA, there is a need of securing confidential messages from each other in case of untrusted users [11].

To cope up with these security risks, physical layer security (PLS) techniques have emerged as a promising solution that can complement and (in some cases) may even replace the cryptography-based approaches [11] [190]. PLS exploits the dynamic features of wireless communications, for example, random channel, fading, interference, and noise, etc., to prevent the eavesdropper from decoding data while ensuring that the legitimate user can decode it successfully. PLS approaches can be exploited to extract keys from the channel, thus avoiding key management issues. Furthermore, in PLS, channel-dependent resource allocation and link adaptation can be designed to provide flexible and scenario-specific security for 5G and beyond [11].

Based on the potential of PLS for future networks and security concerns in NOMA, designing PLS techniques for NOMA is a promising area of research. However, there is still a paucity of research works in this direction [16] [191]. In this article, we first provide a quick overview of NOMA flavors and basic principles to explain security concerns more clearly. This is followed by security design objectives and solutions provided by PLS. Then, we present the merits of PLS in NOMA as compared to OMA. Challenges of PLS in NOMA, possible solutions, and future directions are addressed in the following section. The final section concludes the article.

10.2 Dominant Flavors and System Model for NOMA

In this section, different types of NOMA, basic system model, and NOMA principles are presented to explain the security designs more clearly.

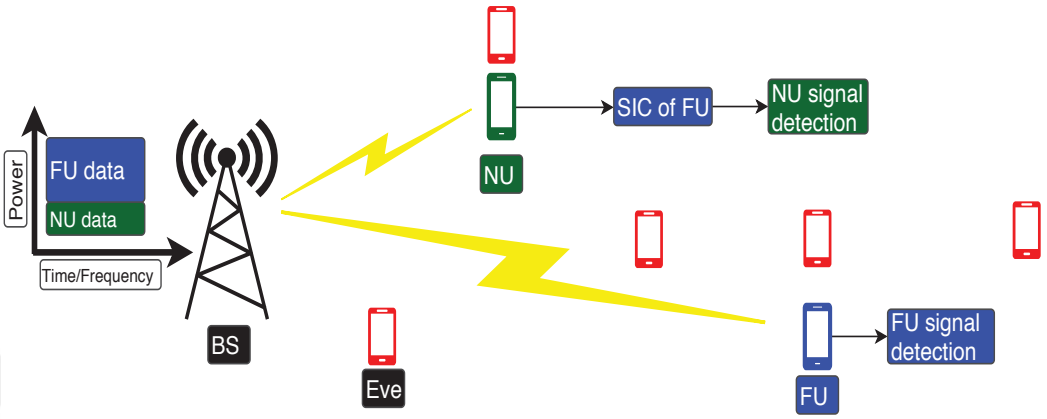


Fig. 10.1: Downlink NOMA detailed model which consists of a single Base Station (BS) with one Near User (NU) and one Far User (FU) in the presence of an external eavesdropper (cloned at different possible positions).

10.2.1 NOMA Dominant Flavors

NOMA supports massive connectivity and enhanced spectral efficiency by allowing resource allocation in a non-orthogonal manner. There are two basic types of NOMA schemes: Power-domain (PD) NOMA and code-domain (CD) NOMA [189]. In PD-NOMA, different users' signals are directly superimposed by assigning channel quality-based power allocation to them, while sharing the same frequency-time resources. CD-NOMA, on the other hand, is like Code Division Multiple Access (CDMA), where different users are allowed to share the same frequency-time resources by using unique orthogonal code. However, CD-NOMA uses non-orthogonal codes with lower cross-correlation or sparse sequences. While uplink NOMA [192] has also been studied, more focus is given to downlink NOMA, especially by the standardization bodies, such as the third generation partnership project (3GPP) and IEEE. For example, a downlink version of PD-NOMA has been proposed for 3GPP-LTE-Advanced [193]. Hence, this paper will mainly focus on PLS techniques applied to downlink PD-NOMA to elaborate on the novel challenges and future recommendations for it.[1]

[1]Note that we will use the term "NOMA" in the remaining part of the paper to represent "PD-NOMA" [189].

10.2.2 System Model and Principles of NOMA

Consider a simple two-user downlink NOMA scenario that consists of a single base station (BS) with one near user (NU) and one far user (FU) in the presence of an external eavesdropper (cloned at different possible positions) as shown in Fig. 10.1. The BS first superimposes the users' signals by allocating them different power levels and broadcasts the mixture to all users using the same time-frequency resources. The power allocation in NOMA is done in such a way that the FU (user with lower channel gain) is allocated more power and NU (user with higher channel gain) is given low power. The receivers of NOMA employ different strategies for different users in accordance with their channel characteristics. More specifically, the NU has to decode the signal intended for FU first, and afterward, it subtracts the detected signal from the received signal and then decodes its intended data. This process is known as successive interference cancellation (SIC). On the other hand, the FU directly decodes its information while considering the information of its partner as noise. It should be noted that for the sake of explanation two users case is considered here; however, the discussion is also applicable to multiple (more than two) users case. The above-mentioned case is for single-input-single-output (SISO)-NOMA, where channels are represented by scalars. However, matrices are used to represent the channels of multi-input-multi-output (MIMO)-NOMA. In the case of matrices, ordering of users based on power is quite challenging [189]. In the literature, two main designs are proposed for MIMO-NOMA case: 1) *Beamformer based MIMO-NOMA*, where different beams are allocated to different users and SIC is employed at users sharing the same resource block [189], 2) *Cluster based MIMO-NOMA*, where users are divided into clusters and a single beam can serve all the users in the cluster. In this approach, SIC is adopted among users sharing the same cluster [189].

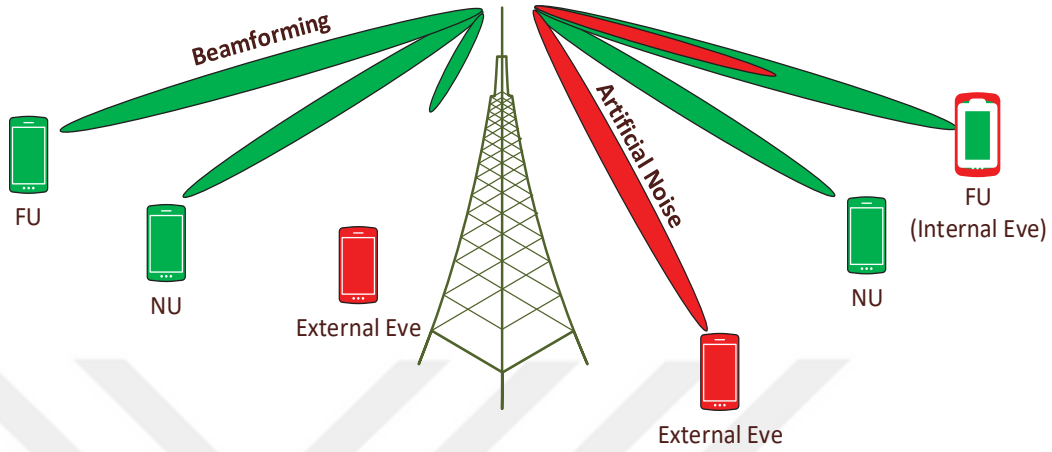


Fig. 10.2: Security based approaches for internal and external eavesdropper based on beamforming and AN.

10.3 Security Designs Objectives

In this section, different security design objectives for NOMA are presented and explained. To evaluate the secrecy performance of any security algorithm, the secrecy rate is one of the popular metrics in PLS. It is defined as the difference between the capacity of the legitimate user channel (main channel) and the capacity of the eavesdropper channel (wiretap channel).

In general, different users in NOMA can have different requirements in terms of reliability, throughput, and security, etc. which implies that the design of PLS techniques should consider these requirements. Moreover, there are two types of eavesdroppers: 1) External, and 2) Internal. An internal eavesdropper is from the set of legitimate users of the network, while the external one is not from that set [190]. The eavesdropper can be considered 1) active, or 2) passive. The active eavesdropper can interrupt wireless communication by launching jamming or channel estimation attacks while passive eavesdropper just spies on the communication without interfering with the ongoing communication.

This work is focused on both internal eavesdropping as well as passive external eavesdropping. The objectives of security design for NOMA can be divided into three major categories based on its requirements as follows:

- Security designs against external eavesdroppers.
- Security designs against internal eavesdroppers.
- Security designs against both internal and external eavesdroppers.

The details of security designs and solutions provided by PLS are presented in the subsequent part.

10.3.1 Security Designs against External Eavesdroppers

In this scenario, NU and FU are trusted. So, the design goal here is to secure the messages of NU and FU from an external eavesdropper. Based on the basic model presented in Fig.10.1, there are different possibilities for Eve's location. In some cases, Eve is closer to BS compared to users, and her channel is better than far legitimate users. Hence, the location of Eve can affect the security performance of NOMA system and should be considered while designing security algorithms. Moreover, different users are allocated different power levels, due to which they are protected in an unequal manner with respect to Eve's location. More specifically, Eve can eavesdrop their signals to different extents.

The necessary conditions that need to be taken into consideration while designing algorithms for this scenario are as follows: **Firstly**, the basic SIC should be normally operated with the security algorithm, which means that the proposed algorithm should not affect the basic SIC process and the performance of normal NOMA. **Secondly**, the algorithm is also expected to work even in the case of having strong spatial similarity between channels of legitimate and illegitimate parties.

The popular PLS techniques for external eavesdropping in the literature include channel-based optimization of the power allocation for each user, subcarrier assignment to users, channel ordering of NOMA users along with the decoding order, optimization of beamforming policies, adding interfere signal, key generation, phase manipulation, transmit antenna selection (TAS) approaches and inter-user

interference exploitation, etc. [11] [16]. The brief details of popular approaches are as follows:

10.3.1.1 Beamforming

The basic idea of the beamforming-based security approach in OMA is to enhance the power of the signal at the legitimate users while suppressing it in other directions [11] as presented in Fig. 10.2 (left). However, this approach may not be able to fulfill the above-mentioned design requirements for secure NOMA. For example, the beamforming design matrices based on maximum ratio transmission for near and far users increase the strength of both users' signals which may not guarantee perfect SIC processing at near user [194]. Hence, these techniques need to be intelligently modified.

10.3.1.2 Artificial noise (AN) with beamforming

AN based techniques with beamforming are very effective against external eavesdropping in NOMA, especially when Eve is closer to BS compared to the legitimate user. The basic idea is to transmit intentional interference simultaneously with the desired signal by using the beamforming approach to degrade the performance of eavesdropper while fulfilling the above mentioned basic security design requirements for NOMA as presented in Fig. 10.2 (right bottom). The performance of such types of techniques is highly dependent on the availability of channel state information (CSI) of the eavesdropper. In the case of full CSI availability at the BS, optimal and efficient beamformers can be designed to enhance the security [16]. However, when CSI is not available, the beamformer should be designed to send AN in all directions except in the direction of the desired user while sending the intended signal in the direction of the desired user [194]. The major challenge here is to ensure secure communication while fulfilling the above-mentioned conditions.

10.3.1.3 Power allocation

Power allocation approaches based on channel conditions of legitimate users can make the interception of users' signals difficult for eavesdropper under certain settings in NOMA [195]. In the case of full CSI availability, the power allocation can be optimized to maximize the secrecy rate (security) of the legitimate users [195]. However, in the case of imperfect CSI, optimal power allocation for maximizing secrecy rate (security) is not possible [16]. So, in such cases, the goal is to maximize the difference in data rate between Eve and users as much as possible.

10.3.1.4 Cooperative beamforming and jamming

Cooperative communication can enhance the reliability of NOMA systems by cooperative diversity. Moreover, it can also enhance the security of the NOMA system by distributed beamforming with and without cooperative jamming. In the case of distributed beamforming, the signal is directed towards the desired direction by collaborative action of relays [196]. On the other hand, in case of distributed beamforming with cooperative jamming, a group of relays is selected to focus the desired signal in the intended direction while the remaining relays are used to degrade the performance Eve by sending AN [196].

10.3.2 Security Designs against Internal Eavesdroppers

In this scenario, no external eavesdropper is assumed; however, the users are untrusted. The design goal here is to secure information of users from each other, while making sure that the SIC operation works normally. Moreover, in this case, the channel is known at the BS, which makes the design process different than the previous case. Internal eavesdropping can be divided into two types:

- Eavesdropping of FU by NU

- Eavesdropping of NU by FU

10.3.2.1 Eavesdropping of FU by NU

In the basic NOMA principle, the main security risk for FU is that the NU has to decode (or demodulate) the signal of FU in order to apply SIC. Another important thing is that the FU's signal is allocated more power, which makes its detection easier for the NU. The design goal here is to avoid leakage of information of FU to NU, while making sure that SIC works normally. To further elaborate on this issue, it should be pointed out that there are two types of SIC receiver: The first one is **symbol-level SIC receiver**, in which FU's signal is demodulated but not decoded in order to apply SIC, while the other one is **codeword-level SIC receiver**, where FU's signal is demodulated and decoded in order to apply SIC. In the codeword-level-SIC case, the data can only be secured by cryptography-based techniques. However, for the case of symbol-level-SIC, PLS techniques can be applied. In symbol-level based SIC, security can be provided to FU's data by transforming its data into another domain by using a special sequence such that NU can apply SIC normally, but cannot decode the information of FU [197]. Moreover, this transformation can also be done by using channel-dependent features. Note that there are not too many contributions to the literature in this direction.

10.3.2.2 Eavesdropping of NU by FU

In the basic NOMA principle, the FU can decode its signal directly, considering the information of near as noise. However, after obtaining its own signal, it may detect the signal of NU. The design goal here is to secure the data of NU from FU while making sure that SIC works normally. In this case, designing security methods is easier as compared to the security problem of FU's data. The BS can employ PLS techniques based on power allocation, beamforming, or any other adaptation-based algorithm to satisfy the security requirement of NU while making sure that the basic data rate requirement of FU is fulfilled.

For example, in the case of beamforming, the design should consider the balance between ensuring security at the near user while reliability at the far user, as presented Fig. 10.2 (right top).

10.3.3 Security Designs against both Internal and External Eavesdroppers

In this scenario, there is an external eavesdropper as well as an internal eavesdropper where the users in the network are not trustable. The design goal here includes the security of signals intended for NU and FU from external eavesdropper as well from each other. This case is the most challenging one with respect to security design. The design algorithms should make sure that SIC will work normally while fulfilling the above goals. One possible way to provide security, in this case, can be by the transformation of the signal of near and far users into another domain by using some randomization sequences [197]. However, this is still an open research area, and a lot of research efforts are needed in this direction. A summary of the objectives of security designs, complexity, and popular solutions for NOMA are presented in Table. I.

10.4 Merits of PLS in NOMA

In this section, we present some of the merits of NOMA over OMA with respect to PLS under certain conditions.

10.4.1 Higher Sum-Secrecy Rate

In NOMA, the signals are not sent separately like OMA. Hence, multi-user interference and PLS can be processed collaboratively. Moreover, user selection,

Table 10.1: Summary of the objectives of security designs for different scenarios in NOMA focusing on passive External Eavesdropper and Active internal eavesdropper.

Scenarios for security	**Design objectives**	**Design Complexity**	**Candidate solutions**
External Eavesdropper	Securing NU and FU data against external Eavesdropper while keeping normal SIC	Normal	Beamforming, Power allocation based, interference exploitation based, TAS, cooperative communication, etc.
Internal Eavesdropper	Securing users' information from each other while ensuring normal SIC	**Against NU**: High **Against FU**: Normal	**Against NU**: Transformation of FU to other domain **Against FU**: Beamforming Power allocation, TAS etc.
External and Internal Eavesdropper	Securing users' information from each other as well as from external Eve while having normal SIC	Highest	Transformation of users' signal into another domain, interference assisted, etc.

number of clusters, intra-cluster and inter-cluster power allocation can be designed based on the quality of service requirements of legitimate users such as data rate, reliability, etc. to enhance the secrecy rate of the system. For example, power allocation based on channel conditions of legitimate users can enhance the security of the system under certain settings as presented in Fig. 10.3 of [195] . It should be noted from the figure that the average sum secrecy rate (ASSR) of the NOMA system improves with the increase in the number of users as compared to OMA under specific settings. The reason for the improvement in ASSR is due to the dominance of legitimate users' high spectral efficiency [195].

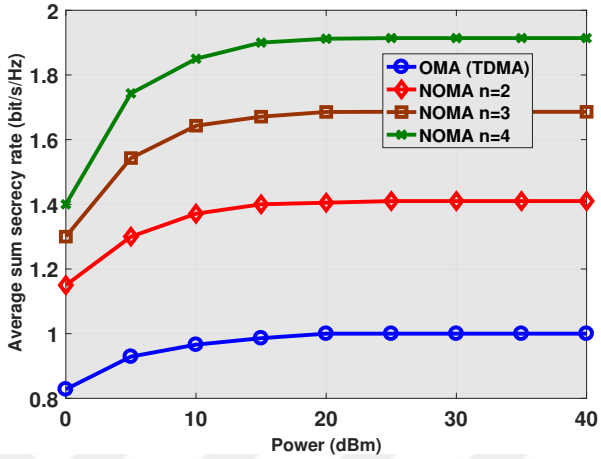


Fig. 10.3: Average Sum Secrecy Rate (ASSR) versus the transmit power for different number of users (n=2, n=3, n=4).

10.4.2 Inter-User Interference Exploitation for Securing Massive MIMO System

In the case of a massive MIMO system, AN-based security techniques face complexity issues. In such cases, NOMA can help us to provide secure communication without using AN [4]. For example, consider a clustering-based Massive MIMO NOMA system employing non-orthogonal channel estimation in the presence of multiple active eavesdroppers [4] as presented in Fig. 10.4. The nodes in this system suffer from intra-cluster and inter-cluster interference; however, this inter-user interference can be exploited intelligently in NOMA to provide secure communication [4]. More specifically, power allocation coefficients during channel estimation and multiple access stages can be designed in such a way that it will enhance the performance of legitimate users and degrade the performance of active eavesdroppers [4]. Moreover, this approach can also be extended to full-duplex NOMA to provide secure communication [16].

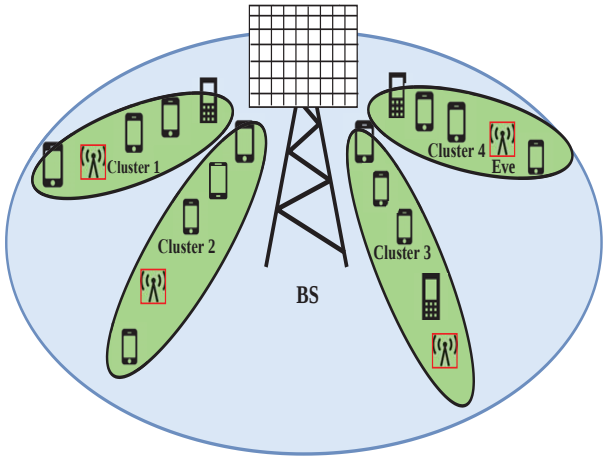


Fig. 10.4: Secure massive MIMO with NOMA by using inter-user interference, where users are divided into four clusters [4].

10.4.3 Securing Uni-Cast Message from Multi-Cast Receivers

An interesting advantage of NOMA is to secure a uni-cast message from interception by the untrusted multi-cast receivers while improving spectral efficiency [5] as presented in Fig. 10.5, where uni-cast message is for a specific receiver while the multi-cast message is for all the receivers in the set of specific receivers. In OMA, uni-casting and multi-casting are transmitted separately and can be intercepted easily by multi-casting receivers as presented in Fig. 10.5. However, the NOMA principle can be used to degrade the intercepting capabilities of the multi-casting receivers similar to the case of securing NU message from untrusted FU receiver [5]. More specifically, joint power allocation and beamforming strategies can be used to enhance the secrecy of uni-cast message while preserving the reliability of multi-cast message [5]. Moreover, in OMA, two slots are required to send uni-casting and multi-casting information while in NOMA both information types can be transmitted simultaneously by using a single slot [5] as presented in Fig. 10.5.

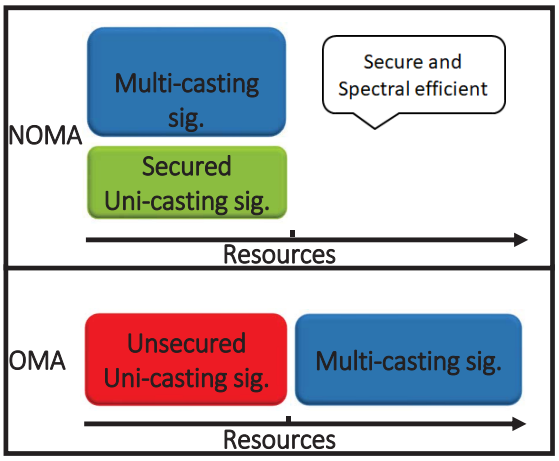


Fig. 10.5: Multi-casting and Uni-casting in NOMA and OMA [5].

10.4.4 Channel Correlation and Security

Most, if not all, PLS techniques (based on small scale fading) assume that the received signals at Eve and Bob will experience independent fading if they are roughly half a wavelength apart. This assumption is valid only in a sufficiently rich scattering environment. In the case of a poor scattering environment, these algorithms will not ensure secure communication. However, NOMA with large scale fading based security algorithms can provide secure communication under certain circumstances even in a poor scattering environment [191] [4]. Moreover, in the case of a rich scattering environment, both the small and large scale fading based security algorithms can be applied in NOMA.

10.5 Challenges and Future Research Directions

This section presents the challenges in securing NOMA using PLS alongside some of the proposed solutions and research directions.

10.5.1 Challenges for Security against FU and External Eavesdroppers

There are considerable contributions in the literature regarding the provision of secure communication schemes against untrusted FU and external eavesdroppers (in case of trusted internal users), such as channel-dependent power allocation, beamforming, cooperative communication, TAS and inter-user interference, etc.. However, the majority of the research works assumes the availability of full, partial or statistical information about the CSI of Eve, which is difficult to achieve in case of passive eavesdropping. Moreover, some techniques provide security at the cost of performance degradation. Hence, conventional techniques should be intelligently modified, and novel techniques should be proposed to provide security for NOMA. Some of the potentially interesting techniques like multi-dimensional directional modulation scheme, cyclic feature suppression-based techniques, and channel-based interleaving, etc., have not been explored for such cases, whereas these techniques have the potential to be used in such situations [16].

10.5.2 Security Challenges against Untrusted NU and both External and Internal Eavesdroppers

The design of security algorithms against untrusted NU and both internal and external eavesdropper is extremely challenging. The only solutions available in the literature so far are based on the transformation of signals into another domain. This transformation is done by using a transformation sequence that needs to be shared between the legitimate parties [197]. The sequence can be shared by PLS approaches, such as full-duplex jamming based techniques for sequence sharing [197] which requires complex hardware. In this direction, the channel-based phase manipulation of symbols, directional modulation and cross-layer security techniques can also be effective. For example, automatic repeat request (ARQ) with AN can be jointly designed to provide security against internal and external eavesdropping in NOMA similar to the work presented in [198]. Moreover, joint

composite constellation design and ARQ with adaptive modulation can also be used to provide security against untrusted NU. Furthermore, in the case of a rich scattering environment, channel-based manipulation security techniques can also be employed in such scenarios. This is still an open area and a lot of research efforts are needed to provide security for such cases while making sure the SIC operation works normally.

10.5.3 Passivity and Limited Observations

A lot of techniques in the literature of secure NOMA consider that the illegitimate user is just spying the information. However, in future networks, there may exist illegitimate nodes that can interfere with the normal operation of the NOMA system by active attacks, such as pilot spoofing attacks, etc. These attacks are more critical in NOMA because of the broadcast of superimposed messages of multiple users at the same time. Quite a few PLS techniques in the NOMA literature are robust to active eavesdroppers' case [4]. Hence, there is a need of designing PLS techniques that are robust to active attacks from eavesdroppers. Moreover, collaborative-eavesdroppers with multiple observations may lead to zero secrecy rate [190]. Hence, there is a need for understanding the implications of collaborative-eavesdroppers and multi-observation cases while developing security techniques for NOMA.

10.5.4 SIC and Eve Capability

In the literature, it is assumed that eavesdroppers use the same SIC procedure as legitimate users. However, an eavesdropper can apply alternative strategies for eavesdropping, for example, it may decode a signal in the first step that is decoded in the last stage of SIC at legitimate users, which can affect the overall security performance of the system. Moreover, a powerful eavesdropper can apply parallel interference cancellation to simultaneously decode the users' signal [189]. Possible alternative approaches by eavesdropper should also be considered while

designing security algorithms.

10.5.5 SIC Error Propagation and Secrecy

The security algorithms in NOMA mainly rely on the assumption that perfect channel estimate is available, and the signals are perfectly separated at the receiver side (perfect SIC). However, if there is an error in any of these signals during SIC, then the remaining signals may also be detected erroneously [199]. Hence, the effect of imperfect SIC and imperfect channel estimation should be considered while designing security algorithms for NOMA, so that these drawbacks can be avoided. Therefore, it is also recommended to use an efficient non-linear detection algorithm at each state of SIC to alleviate the effect of imperfect SIC and practical channel calibration solutions for imperfect channel estimation case. Moreover, new interference cancellation schemes and improvement in signal processing chip technology that can benefit the legitimate receivers are also of special interest [189].

10.5.6 AN based Security Schemes

AN-based techniques are one of the popular techniques in the literature. In these techniques, an artificial interference signal is added in the null-space of the legitimate user channel to degrade the performance of Eve. However, in NOMA, when AN is added based on the individual user, it also causes AN leakage in the range space of other NOMA users which degrades their performance. Moreover, AN may increase peak to average power ratio (PAPR), sacrifices some power, and is also sensitive to imperfect channel estimation. Thus, it is recommended to design AN, not only to provide security but also to reduce the amount of out-of-band emission (OOBE), adjacent channel interference and average PAPR, etc. [198].

10.5.7 Multi-Cell Case and Other Technologies

In the case of multi-cell NOMA, there are a lot of challenges to provide secure and reliable communication due to inter-channel interference. However, there is not much work in this area. Algorithms for joint processing, coordinated beamforming, and coordinated scheduling need to be proposed to ensure reliable and secure multi-cell NOMA. Moreover, there is also the paucity of PLS research works for NOMA integrated with other technologies such as millimeter-wave, full-duplex, visible light communication, cognitive radio, heterogeneous networks, and coordinated multi-point, etc.

10.5.8 Cross-layer, Context-Aware and Hybrid Security Techniques for NOMA

In the literature of PLS techniques in NOMA, transmission parameters of the physical layer are optimized according to legitimate users' channel characteristics to provide secure communication without considering upper layer parameters. However, to meet the diverse requirements of NOMA users and for joint design of throughput, secrecy, delay, reliability, and respective trade-off among them, the concept of cross-layer security design from the perspective of physical layer should also be considered such as: 1) Cross MAC-PHY layer: In this approach, MAC layer features (for example, channel accessing, multiplexing, ARQ and control of resource allocation, etc.) can be optimized jointly with physical layer parameters to provide efficient QoS based security solution [198], 2) Cross NET-PHY layer security: In this approach, the network layer features such as relaying, routing and path determination, etc. can be optimized jointly with physical layer parameters for enhancing security of the system [190], 3) Cross APP-PHY layer: In this approach, physical layer parameters of transmission are jointly optimized based on channel characteristics as well as on the basis of applications, services and features of data to provide efficient security solution based on the requirements of users. Finally, designing **hybrid** techniques by combining signal's security approaches (PLS) with data security approaches (cryptography) can further enhance the

security of the NOMA-based systems.

10.5.9 IRS assisted PLS for NOMA

Recently, reconfigurable intelligent surfaces (RIS)-assisted networks have been proposed as a promising power-efficient solution to enable a smart and controllable wireless propagation environment. Basically, the RIS is a large array of passive reflecting elements that intelligently reflect the impinging signals in order to add different signals constructively or destructively at receivers [200]. This feature can be exploited to enhance PLS against external and internal eavesdropper in NOMA.

10.6 Conclusion

NOMA promises high spectral efficiency, low latency, and massive connectivity, while PLS offers simple and effective security solutions. Together, these two technologies are capable of supporting the exceeding efficiency and security requirements of 5G and beyond networks. In this article, the key security design requirements of NOMA and the strength of PLS as a solution to fulfill these requirements are discussed. By employing PLS to NOMA, spectrally efficient, adaptive, and secure systems can be realized. However, the challenges and future recommendations explained in this work need to be investigated further to address the open issues. Practical secure NOMA systems can be developed by modification of current PLS techniques and/or proposing new novel techniques that do not require extra processing, extra signaling, or major modification in the receiver structure.

Chapter 11

Primary User Emulation and Jamming Attack Detection in Cognitive Radio via Sparse Coding

11.1 Introduction

Due to the rapid growth in wireless technology and services, the scarcity of the wireless spectrum has become a major problem [201]. To meet the requirements of future wireless networks and to alleviate this spectrum scarcity problem, cognitive radio (CR) is one of the most promising solutions. CR allows spectrum sharing between the primary users (PUs) and secondary users (SUs). More specifically, it enables SUs to opportunistically utilize empty spectrum bands without harming the PUs by following these steps: i) determining whether the channel is occupied or not, ii) choosing the best part of the spectrum based on their quality of service (QoS) requirements, iii) coordinating with other users to access the spectrum, and iv) leaving the channel whenever a PU starts to transmit its data [202].

Although CR is a promising solution to address the spectrum shortage problem, it is inherently vulnerable to both traditional and new security threats [203]. This is due to the wireless nature and unique characteristics of CR. Traditional security threats include eavesdropping, spoofing, and jamming attacks [204], while new security threats include spectrum sensing data falsification (SSDF) and primary user emulation attack (PUEA) [203, 205].

An eavesdropper tries to "hear" the secret communication between legitimate nodes while a spoofer can modify, intercept, and replace the messages between the legitimate parties. On the other hand, a jammer can generate intentional interference signals to degrade the quality of communication for both PUs and SUs. Thus, a jammer can also prevent an SU from efficiently utilizing the white spaces of the spectrum by causing false alarms regarding spectrum occupancy [204].

In an SSDF attack, an illegitimate node provides false sensing information to degrade the performance of the collaborative spectrum sensing approach, where collaborative approaches include the interaction of multiple CRs to improve the sensing performance in the fading environment. On the other hand, PUEA is based on emulating the characteristics of the PU transmission to deceive the SUs about spectrum occupancy. PUEA prevents them from utilizing the existing spectrum holes and can even cause interference to the PUs in some cases [206].

Popular PUEA types include malicious and selfish attacks. The malicious attackers' objective is to degrade the CRs performance by preventing them from opportunistic exploitation of spectrum. Particularly, a malicious attacker destroys the operations of the CR network. Thus, it can stop CRs from sensing and can also disengage the already used spectrum by them. On the other hand, a selfish attacker aims at exploiting the space of the spectrum by preventing other secondary users from using it. More specifically, it focuses on enhancing its consumption of the spectrum by degrading the overall fairness of the system.

The focus of this work is to detect false alarm about the spectrum occupancy that is caused by illegitimate nodes. An illegitimate node can transmit a signal

similar to that of a PU, considered as a primary user emulator (PUE), or can send an unstructured signal, considered as a jamming attack. In the literature, several solutions are proposed for illegitimate node detection. For instance, the power level of the signal through the energy detection (ED) algorithm can decide on the source of the signal [207] using a pre-defined threshold. In [208], the authors presented a Markov random field-based belief propagation framework with ED for PUEA detection. Firstly, SUs employ the energy-based algorithm and calculate the belief values about the real source of the signal. Afterwards, the belief values are shared between different users. Finally, the average belief value is compared with the pre-defined threshold. If the average is less than the threshold, it is assumed that the signal source is fake, otherwise, the source of the signal is assumed to be real. These approaches are simple, however, they are shown to create high levels of false alarm rates. Cross-layer techniques are also effective for illegitimate node detection. In [209], the authors proposed a cross-layer approach for jamming attack and PUEA detection in CR networks by using information from physical layer spectrum sensing, statistical analysis of routing information, and prior knowledge about PUs. This technique is effective for detecting PUEA and jamming attack. However, there is an excessive overhead in analyzing and comparing information from physical and network layers.

The wireless channel and inherent physical characteristics of communication devices are also effective for illegitimate node detection [210–213]. For instance, wireless channel-based detection schemes are proposed in [210–212] for PUEA detection. These techniques are based on the fact that the channel between different transmitter-receiver pairs is different due to its spatial decorrelation nature. In [213], the inherent physical layer features of devices based on hardware impairments are exploited for PUEA detection. Nevertheless, these techniques require excessive software and hardware overheads for their implementation.

Localization-based detection is also popular for PUEA detection. The basic idea is to infer the position of the signal's source by using the received signal and compare it with a database of pre-known locations of legitimate PUs. However, database management is not applicable in all scenarios [214, 215]. Similarly, the authors in [216] used the time difference of arrival-based position estimation

approach for PUEA detection. However, this requires a strict synchronization between the receiver and the transmitter.

Machine learning (ML)-based solutions also received considerable attention for CR security. In [217], an anomaly detection framework for CR networks based on the characteristics of radio propagation is proposed. However, it does not consider specific attacks and is designed only for the detection of general anomalies. In [218], the authors proposed a technique based on support vector data description (SVDD) and zoom fast Fourier transform (zoom FFT). In the first step, the pilot and symbol rate are estimated using zoom FFT. Afterwards, a boundary around the PU objects is constructed using the SVDD classifier which is used to distinguish between PU and PUE. However, this method does not perform well in low signal-to-noise ratio (SNR) operating conditions. Furthermore, the method fails when the PUE is extremely intelligent (the only information unknown by the PUE is the channel). In [219], the authors proposed an ML-based algorithm for PUEA detection that exploits the signal strength and boundaries around the position of PU for the correct detection. This method is good in terms of complexity but it suffers from performance degradation.

Recently, compressive sensing (CS)-based approaches were applied in spectrum sensing where CS offers several benefits. For example, it can alleviate the need for high sampling rate analog-to-digital converters [220–222]. This results in a reduction of the overall complexity, energy consumption, and memory requirements. Following its success in various application areas [220], CS has been applied to the problem of PUEA detection. Works along this line include PUEA detection based on CS and received signal strength [223]. This approach needs multiple sensors throughout the network. Hence, it increases the overall complexity. Another example considers exploiting belief propagation and CS for PUEA detection [224]. However, this requires a centralized node for its implementation. In [225], the authors proposed an algorithm for jamming attack detection in wide-band CR. In the first step, CS is performed to estimate a wide-band spectrum. Afterwards, an ED algorithm is applied to identify the occupied spectrum sub-bands. Lastly, waveform parameters of the sub-bands are compared with the known user database to determine the jamming attack. However, this method

also requires database management.

In this paper, we propose an algorithm for PUEA and jamming attack detection corresponding to the narrow-band spectrum using the convergence patterns of the sparse coding over channel-dependent sampled dictionary. This convergence is characterized by the sparse coding residual signal energy decay rates. The proposed algorithm does not require a centralized node or strict synchronization between transceiver ends. Moreover, it does not require information from multiple sensors for the implementation. Furthermore, it eliminates the need for estimating the sparse coding error tolerance or the sparsity level, as typically required in CS-based approaches. The reason is that the sparse recovery in the proposed algorithm is just used for energy convergence rate revelation rather than accurate signal reconstruction. The main contributions of this paper are as follows:

- First, the decaying pattern of sparse coding is used for PUEA detection. This is achieved by exploiting the convergence patterns of the sparse coding over a PU channel-dependent dictionary. In this context, these patterns guide on identifying a spectrum hole, a PU, and a PUE through ML approaches.
- Second, jamming attack detection is also performed based on the decay pattern of sparse coding. Here, the idea is that the noise and jamming signals are not compressible because they are not structured. So, residual energy decay patterns with a channel-dependent dictionary along with the non-compressive nature of jamming signals are used for efficient jamming attack detection via ML classification.

Notation: Upper-case bold-faced, lower-case bold-faced and lower-case plain letters represent matrices, vectors, and scalars, respectively. The symbols $\|.\|_0$ and $\|.\|_2$ denote the number of nonzero elements and the 2-norm of a vector, respectively. The $\langle\cdot,\cdot\rangle$, $\dagger$, and $\mathbb{C}$ symbols represent inner product, Moore-Penrose pseudoinverse, and complex number field.

11.2 Preliminaries and System Model

This section reviews background information related to CS, sparse recovery, and ML approaches.

11.2.1 Compressive Sensing and Sparse Recovery

Using a random sensing matrix, CS merges data measurement and compression into a unified operation. CS applies to compressible signals, i.e., either the explicitly sparse signals, or the ones admitting sparsity in a certain domain [226].

Let us assume a signal vector $\boldsymbol{y} \in \mathbb{C}^N$. A compressed version of $\boldsymbol{y}$ can be obtained by applying a measurement matrix $\boldsymbol{\Phi} \in \mathbb{C}^{M \times N}$ as $\boldsymbol{y_c} = \boldsymbol{\Phi y}$, where $M \ll N$. Hence, a reduction in dimensionality from N-to-M is achieved. A high-dimensional version of the original signal can be reconstructed from this low dimensional measurement via sparse recovery [226].

Generally speaking, let us assume that a signal $\boldsymbol{y}$ admits sparse coding over a dictionary ($\boldsymbol{D} \in \mathbb{C}^{N \times K}$). The signal can be represented in terms of $\boldsymbol{D}$ as $\boldsymbol{y} \approx \boldsymbol{Dw}$, where $\boldsymbol{w} \in \mathbb{C}^K$ is a sparse coefficient vector. The calculation of $\boldsymbol{w}$ can be cast as follows.

$$\underset{\boldsymbol{w}}{\operatorname{argmin}} \|\boldsymbol{y} - \boldsymbol{Dw}\|_2^2 \; s.t. \; \|\boldsymbol{w}\|_0 < S, \tag{11.1}$$

where S denotes the sparsity level of the signal. Sparse recovery is an NP-hard problem. However, sparse recovery methods offer efficient approximate solutions. As shown in (11.1), the ℓ_0 pseudo-norm is principally used to exactly quantify the sparsity level. However, its minimization is mathematically intractable and highly complex. Therefore, there exist only approximate solutions to ℓ_0 minimization, such as the matching pursuit and orthogonal matching pursuit (OMP) approaches. Alternatively, this problem can be overcome by relaxing the ℓ_0 norm minimization condition to minimizing the ℓ_1 norm which is a loose bound on sparsity. Still, ℓ_1 minimization is convex and accepts linear programming. Thus, replacing ℓ_0 minimization with ℓ_1 minimization offers a significant reduction to

the computational complexity of sparse coding. However, ℓ_1 minimization requires information about the noise level of the signal being recovered. Thus, in this work, we adopt approximate ℓ_0 minimization through the OMP algorithm [1].

The intrinsic sparsity of the signal can be revealed by a dictionary. This dictionary can be formed of fixed basis functions such as Fourier basis, Gabor functions, wavelets, and contourlets. Alternatively, it can be generated as a learned dictionary. In this setting, a dictionary is obtained by training over training data signals $\boldsymbol{Y} \in \mathbb{C}^{N \times L}$ [228]. This dictionary learning process can be formulated as

$$\underset{\boldsymbol{W},\boldsymbol{D}}{\operatorname{argmin}} \|\boldsymbol{W}_i\|_0 \; s.t. \; \|\boldsymbol{Y}_i - \boldsymbol{D}\boldsymbol{W}_i\|_2^2 < \epsilon \; \forall \;\; i, \tag{11.2}$$

where ϵ represents error tolerance. Since the problem is non-tractable and non-convex, most of the dictionary learning algorithms perform the learning by iteratively alternating between a sparse representation stage and a dictionary update stage. As an example, the K-SVD algorithm [228] is one of the widely used algorithms for the dictionary learning process.

The above-mentioned dictionary learning is a computationally demanding process. Therefore, developing efficient alternatives to the classical dictionary learning approach is needed for CR-related applications [221]. In this context, the use of sampled dictionaries is an efficient alternative. One can obtain a sampled dictionary by picking a set of randomly-selected data vectors that serve for the sparse coding without the need for applying an expensive learning process. Thus, this offers a compromise in terms of computational complexity at a tolerable loss in the representational power of the dictionary. In [222], the use of sampled dictionaries is justified by their usage to represent data points in a specific class, which have a general similarity. Similarly, sampled dictionaries are used in this work to represent signals.

[1] The proposed algorithm is not limited to OMP and it can be implemented with any sparse recovery algorithm [227]. We prefer to use the OMP algorithm since it is computationally efficient and simple.

11.2.2 Residual Components in Pursuit Sparse Coding

A widely used sparse representation algorithm is OMP. This algorithm is based on iteratively obtaining the coefficients in a sparse coefficient vector ($\boldsymbol{w}$). Particularly, each iteration identifies the location and adjusts the value of a nonzero element in $\boldsymbol{w}$. This is achieved by selecting one atom (column) from a dictionary $\boldsymbol{D}$ and adjusting its respective weight.

To implement the above-explained atom selection and coefficient update processes, algorithms such as OMP define a so-called residual signal $\boldsymbol{r}$. Conceptually, $\boldsymbol{r}$ represents signal portions that have not yet been represented by the selected dictionary atoms. Hence, sparse coding initializes $\boldsymbol{r}$ with the signal itself, as $\boldsymbol{r} \leftarrow \boldsymbol{x}$. In the first iteration, the sparse representation algorithm loops through all dictionary atoms and selects the one most similar to the current residual $\boldsymbol{r}$. Once this atom is selected, the corresponding weight is calculated. To this end, the next residual is calculated by subtracting the resultant one-atom sparse approximation from the original residual. Then, the residual is considered as a new signal for which another dictionary atom is selected and another coefficient is calculated and the process continues until a certain halting condition is met.

The interesting point to consider in the above-explained sparse coding approach is that the energy of the residual components should dramatically decrease as sparse coding progresses. Intuitively, this is because more atoms are selected, and thus more signal portions are excluded from the residual.

11.2.3 Machine Learning for Classification

The successful works of the ML algorithms in many application areas such as computer vision, fingerprint identification, image processing, and speech recognition led these algorithms to become appealing for the area of wireless communication [229]. These ML algorithms are categorized under three categories called supervised, unsupervised, and reinforcement learning. Supervised learning-based

ML algorithms are widely used for classification problems when the number of present classes is known and the information of the classes that samples belong to in the training stage is available.

Amongst many supervised learning-based algorithms, the feed-forward neural network has received growing interest in classification problems since it can recognize classes accurately and quickly [230]. This network can be used with a single-layer and multi-layer. Although single-layer algorithms are computationally good, these algorithms can only be used for simple problems. Alternatively, the multi-layer-based algorithms that include the usage of one or more hidden layers are used. Even though these algorithms increase computational complexity, they are able to solve more complex problems. Besides the effect of the extra layers, the number of neurons that are used in hidden layers is also effective on the accuracy and complexity performances. Therefore, it is quite significant to set these hyper-parameters optimally. Moreover, the complexity and accuracy performances can be increased by feature extraction (with the domain knowledge). Along this line, CS is used to extract features in this work with the aim of increasing the performance of the ML.

11.2.4 System Model

The system model used is intended to characterize the existence of legitimate and illegitimate source nodes. Thus, it consists of a PU node, an SU node, and an illegitimate node as presented in Fig. 11.1. In this setting, an SU node opportunistically exploits the spectrum in the presence of an illegitimate node that can launch either PUEA or jamming attack. A jammer transmits a random signal, while a PU node and a PUE transmit structured signals that mimic the legitimate PUs.

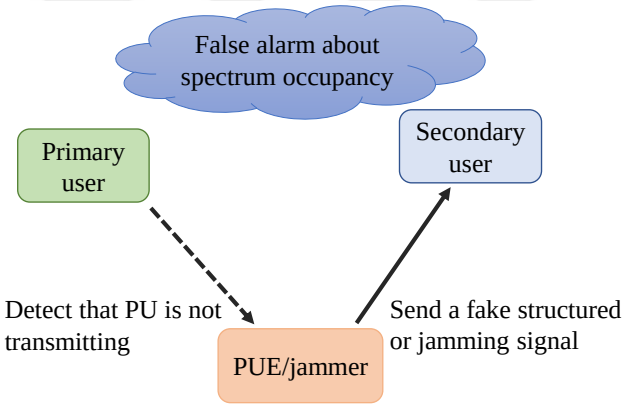
We can represent the transmitted signal as: $\boldsymbol{x} = \boldsymbol{A}\boldsymbol{s}$, where $\boldsymbol{A}$ is a coefficient matrix with a size of $N \times N$. Each component is denoted by $a_{i,j}$ with $i, j = 1, \ldots N$, and $\boldsymbol{s} = [s_1(t), \ldots, s_N(t)]^T$ represents the transmitted data vector. Any coordinate of $\boldsymbol{s}$ is given as $s_i(t) = \sum_{k=-\infty}^{\infty} d_k u(t - kT_s) e^{j2\pi f_{c,o} t}$, where T_s is the

symbol duration, $f_{c,o}$ represents the center frequency, d represents digitally modulated data symbols, $u(t)$ represents the pulse shaping filter, and $o = 1, 2, \ldots, N$.

The signal at the receiver sent by any node can be written as

$$\boldsymbol{y} = \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n}, \tag{11.3}$$

where $\boldsymbol{h}$ is a multipath Rayleigh fading channel between any transmitter-receiver pair and $\boldsymbol{n}$ is additive white Gaussian noise. Due to the spatial decorrelation concept, the channel between different transmitter-receiver pairs is assumed to be different [12].



1.31

Fig. 11.1: The basic system model: a PUE and a jammer want to degrade SU's spectrum utilization by sending fake signals.

11.3 The Proposed Algorithm for PUEA and Jamming Attack Detection

The objective of this work is to differentiate between the following hypotheses:

$$\boldsymbol{y} = \begin{cases} \boldsymbol{n} & \mathcal{H}_0 : \text{there is no PU}, \\ \boldsymbol{h}_{PU}\boldsymbol{x_s} + \boldsymbol{n} & \mathcal{H}_1 : \text{a PU is present}, \\ \boldsymbol{h}_i\boldsymbol{x_s} + \boldsymbol{n} & \mathcal{H}_2 : \text{a PUE is present}, \\ \boldsymbol{h}_i\boldsymbol{x_n} + \boldsymbol{n} & \mathcal{H}_3 : \text{a jammer is present}, \end{cases} \tag{11.4}$$

where $\boldsymbol{n}$ is additive white Gaussian noise and $\boldsymbol{y}$ is the received signal. Besides, $\boldsymbol{h}_{PU}$ denotes the channel corresponding to the legitimate PU, $\boldsymbol{h}_i$ is the channel

corresponding to PUE or jammer, $\boldsymbol{x}_n$ represents the (unstructured) jamming signal, and $\boldsymbol{x}_s$ is a structured signal. In this work, two goals are set. The first is to detect PUEA, i.e., to differentiate between the $\mathcal{H}_0$, $\mathcal{H}_1$, and $\mathcal{H}_2$ hypotheses. The second goal is to detect jamming attacks, i.e., to differentiate between $\mathcal{H}_0$, $\mathcal{H}_1$, and $\mathcal{H}_3$.

To meet the above-mentioned goals, a compressed version of the received signal is observed by the CS algorithm and its sparse coding is calculated with respect to a PU channel-depended dictionary $\boldsymbol{D}_{PU}$. As detailed in Section 11.2, sparse coding iteratively minimizes the energy of a residual ($\|\boldsymbol{r}\|_2$). For each iteration, we calculate the value of $\|\boldsymbol{r}\|_2$. Then, we quantify the rate of its decay using the gradient operator ($|\boldsymbol{G}|$). It is noted that the speed of this decay depends on the harmony between the received signal and the dictionary.

The convergence profile of this residual or gradient versus iteration can be used to distinguish between the aforementioned hypotheses. The idea behind this approach is that the unstructured signals (noise and jamming) are not compressible, while structured signals are compressible. Hence, different signals have different $\|\boldsymbol{r}\|_2$ and $|\boldsymbol{G}|$ profiles that help to distinguish between different hypotheses. Following the same logic, different signals have different patterns based on the similarity between the dictionary atoms and signals. In other words, residual energy patterns show how much dictionary atoms can guarantee accurate and sparse representation for signals that can also help in distinguishing between various hypotheses. Intuitively speaking, a signal that is compressible in the given dictionary has a faster decay speed compared to other signals. Thus, if the dictionary is channel-dependent, it will also affect the pattern corresponding to $\|\boldsymbol{r}\|_2$ and $|\boldsymbol{G}|$, which can be used also to differentiate between different hypotheses.

To this end, we analyze the usefulness of $\|\boldsymbol{r}\|_2$ and $|\boldsymbol{G}|$ in distinguishing between the aforementioned hypotheses in (11.4) with the following test. We use a test set of 10^3 quadruplets of synthetically-generated received signals ($\boldsymbol{y}$) that correspond to the hypotheses $\mathcal{H}_0, \mathcal{H}_1$, $\mathcal{H}_2$, and $\mathcal{H}_3$, respectively. In other words, one signal is mere noise, the other one is the signal received from the legitimate PU, the third one is a PUE signal that mimics the PU signal, and the fourth one

is an unstructured jamming signal. These signals are generated as described in Section 11.5.

For each quadruplet, we calculate a PU-dependent dictionary ($\boldsymbol{D}_{PU}$) based on the known PU channel ($\boldsymbol{h}_{PU}$). In this work, a channel-dependent dictionary is obtained by convolving a set of randomly selected data ($\boldsymbol{X}$) with the channel corresponding to the legitimate PU. Formally stated, $\boldsymbol{D}_{PU} = \boldsymbol{h}_{PU} * \boldsymbol{X}$, where $*$ denotes convolution. Afterwards, we perform an iterative sparse coding operation on a compressed version of each signal in the quadruplet with $\boldsymbol{D}_{PU}$ while calculating $\|\boldsymbol{r}\|_2$. Next, we calculate the gradient of each residual vector as $|\boldsymbol{G}|$.

The average values of $\|\boldsymbol{r}\|_2$ and $|\boldsymbol{G}|$ in the above-explained test are presented in Fig. 11.2. In view of this figure, it is seen that one can differentiate between the four hypotheses based on $|\boldsymbol{G}|$ and $\|\boldsymbol{r}\|_2$ using ML approaches. For example, the gradient of $\mathcal{H}_1$ has faster decay as compared to $\mathcal{H}_0$, $\mathcal{H}_2$, $\mathcal{H}_3$ as presented in Fig. 2 (f), Fig. 2 (e), Fig. 2 (g), and Fig. 2 (h), respectively. The reason for exhibiting a faster decay is that the received signal in $\mathcal{H}_1$ (corresponding to PU) is the only one compressible in the given dictionary.

Based on the above discussion, we present the proposed algorithm. It is divided into two main stages. First, is a classifier training stage, where one uses a comprehensive set of training signals. We can either concatenate $\|\boldsymbol{r}\|_2$ and its absolute gradient $|\boldsymbol{G}|$ into a unified feature vector or use them separately as classification features. These features are used to make training data sets $\boldsymbol{f}_0^i$, $\boldsymbol{f}_1^i$, $\boldsymbol{f}_2^i$, and $\boldsymbol{f}_3^i$ according to the hypotheses explained in (11.4).

For the case of PUEA detection, the training set contains $\boldsymbol{f}_0^i$, $\boldsymbol{f}_1^i$, and $\boldsymbol{f}_2^i$ corresponding to the hypotheses $\mathcal{H}_0, \mathcal{H}_1$, and $\mathcal{H}_2$, respectively. On the other hand, for the case of jammer detection, the training set contains $\boldsymbol{f}_0^i$, $\boldsymbol{f}_1^i$, and $\boldsymbol{f}_3^i$ corresponding to the hypotheses $\mathcal{H}_0, \mathcal{H}_1$ and $\mathcal{H}_3$, respectively. Afterwards, these training vectors, along with their class labels are fed to the ML training stage, where a classifier model is trained accordingly. The workflow of the training set preparation stage is pictorially described in Fig. 11.3-(a). In this figure, $\mathbf{Y}_n^i$ represents the set of compressed received signals $\boldsymbol{y}_0^i$, $\boldsymbol{y}_1^i$, $\boldsymbol{y}_2^i$ for the case of PUEA

detection or $\boldsymbol{y}_0^i$, $\boldsymbol{y}_1^i$, $\boldsymbol{y}_3^i$ for the case of jamming attack detection. Similarly, $\mathbf{F}_n^i$ represents the set of training vectors.

After classifier training, the testing stage represents the run-time operation of the proposed algorithm. This process is explained in Fig. 11.3-(b). For each incoming test signal, $\boldsymbol{y}$, sparse coding is performed over $\boldsymbol{D}_{PU}$ and feature vector $\boldsymbol{f}$ is obtained. Afterwards, $\boldsymbol{f}$ is fed into the learned classifier. Finally, this classifier will decide on the hypothesis corresponding to the current signal of interest. An analysis of this idea is provided in the Appendix.

11.4 Complexity Analysis

In this section, we roughly quantify the computational complexity of the proposed algorithm. This complexity is primarily required by sparse coding and ML.

The OMP computational complexity at the k-th iteration is $\mathcal{O}(MK + KS + KS^2 + S^3)$ while the overall complexity is $\mathcal{O}(MKS + KS^2 + KS^3 + S^4)$, where S represents the sparsity level [231]. Thus, the overall computational complexity of sparse coding with a sparsity level of M is $\mathcal{O}(KM^2 + KM^2 + KM^3 + M^4)$. This can be simplified as $\mathcal{O}(2KM^2 + KM^3 + M^4)$. Note that sparse coding is used during both the training and the testing phase in the proposed algorithm.

The computational complexity of ML is divided into two main stages which are training and testing. The computational complexity of two-layer neural network per sample is $\mathcal{O}(e(lk + ml))$ for training stage, where e denotes the number of epochs, while k, l, and m represent the number of neurons at the input, hidden, and output layers, respectively. The total complexity of training stage is $\mathcal{O}(ep(lk + ml))$ for p number of samples. Moreover, the computational complexity of training per sample is roughly double as compared to the complexity of testing per sample [232]. It is worth to note that $k = 2M$, since $\|\boldsymbol{r}\|_2$ and $|\boldsymbol{G}|$ are concatenated into a unified feature vector in the simulations.

11.5 Results and Discussion

This section presents numerical experiments to assess the performance of the proposed algorithm comparing it with the ED approach.

11.5.1 Parameter Setting

The simulations are conducted with different modulation settings based on the system model specifications presented in Section 11.2. The modulation types used include quadrature amplitude modulation (QAM), pulse amplitude modulation (PAM), frequency-shift keying (FSK), and phase-shift keying (PSK). Moreover, the proposed algorithm uses a 100×400 dictionary. For each received signal, a channel realization [153] is generated for the PU and uncorrelated channel realizations are generated for illegitimate node based on channel decorrelation concept [12]. The assumed model of $\boldsymbol{h}_{PU}$ is: $\boldsymbol{h}_{PU} = \rho\boldsymbol{h} + (1-\rho)E$, where E represents an independent channel, ρ is the correlation factor and $\boldsymbol{h}$ is Rayleigh fading channel [23]. The details of the simulation parameters are presented in Table 11.1.

We use a standard two-layer feed-forward network [230] for that consists of a hidden layer and an output layer with sigmoid functions. The number of hidden neurons is set to 64 while the number of output neurons is set to the number of elements in the target vector which is 3 (corresponding to the number of classes in PUEA or jamming attack detection). For the case of PUEA detection, the vectors $\boldsymbol{f}_0^i$, $\boldsymbol{f}_1^i$, and $\boldsymbol{f}_2^i$ are used for training. For jamming attack detection, $\boldsymbol{f}_0^i$, $\boldsymbol{f}_1^i$, and $\boldsymbol{f}_3^i$ are used as input vectors. Energy decay rate and gradient vectors $\|\boldsymbol{r}\|_2$ and $|\boldsymbol{G}|$ are used as feature vectors. Here, the dimension of both $\|\boldsymbol{r}\|_2$ and $|\boldsymbol{G}|$ is $1 \times M$. Therefore, the feature vector dimension $1 \times 2M$.

It is noted that we take 4000 samples from each class in the training stage for all cases and 1000 samples from each class in the testing stage for each of the SNR values. Also, the neural network is trained over the SNR values ranging

Table 11.1: Synthetic received signal simulation parameters.

Parameter	Value
Channel Model	Rayleigh
No. of taps	7
Channel Delay Unit	Sample Period
Signal Length	100
Oversampling Rate	10
Pulse Shaping	Square-root-raised-cos.
Raised Cos. Symbol Span	50
Raised Cos. Roll-off Factor	0.2
Correlation Factor	0.9

between -5 dB and 15 dB with a step size of 5 dB.

11.5.2 Performance Analysis

This section presents the performance analysis of the proposed algorithm in terms of confusion matrices, receiver operating characteristics (ROC) curves and area under ROC (AUROC) curves. For the jamming detection scenario, it is assumed that the illegitimate node broadcasts non-structured signals. On the other hand, it is assumed that PUE signal's parameters are identical to that of PU signal.

To examine the performance of the classification, confusion matrices are often used. They present the number of both correctly and incorrectly classified observations. Thus, diagonal elements present the number of those observations correctly classified while off-diagonal elements indicate the number of incorrectly classified observations.

Table 11.2 presents the confusion matrices for the case of PUEA detection for different M and SNR values, where M is the number of samples in the compressed received signal. It is observed from Table 11.2 that the overall performance of the proposed algorithm is satisfactory for PUEA detection, especially at high SNR. Besides, the performance also improves with the increase in the values of M. Table 11.3 presents the confusion matrices for the case of jamming detection

for different M and SNR values. It is seen from the table that the classification accuracy based on the proposed algorithm improves with the increase in M and SNR similar to PUEA case.

It is also observed from Tables 11.2 and 11.3 that the performance of the proposed jammer detection outperforms PUEA detection. This is because the jammer detection benefits from both the non-compressive nature of the jamming signal and the channel-dependent dictionary while the PUEA detection benefits only from the channel-dependent dictionary.

In classification, if a signal belongs class i and is correctly classified in to belong to the same class, then it is said to be as true positive (TP). If it is wrongly classified to belong to a different class j, then it is said to be a false negative (FN). If, however, the signal does not belong to class i and is wrongly classified as such, then it is counted as false positive (FP). Finally, if it does not really belong to i and is classified to belong to i, then it is a true negative (TN). To this end, the true positive rate (TPR) or recall can be defined as $TPR = TP/(TP + FN)$, whereas the false positive rate (FPR) can be defined as $FPR = FP/(FP + TN)$. ROC curves and AUROC curve values show the capability of a classifier to distinguish between different classes. ROC is a probabilistic curve which is plotted with a TPR on the vertical axis and FPR on the horizontal axis. Ideally, the TPR equals 1 and the FPR equals 0. Generally speaking, the closer the ROC curve is to the top-left corner, the better the performance. Similarly, the higher values of the AUROC curve shows better performance. In this work, there are three classes ($\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$ or $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_3$) and ROC curve for each class is plotted separately.

Fig. 11.4 and Fig. 11.5 present a performance comparison of the proposed algorithm with the ED-based ML algorithm for PUEA and jamming attack detection, respectively. In the case of ED-based ML, the energy of the received signals is used for the detection of different hypotheses while using ML structure similar to the one used for the proposed algorithm. It is observed from Fig. 11.4 and Fig. 11.5 that the ROC curves of the proposed algorithm are closer to the top-left

corner compared to ROC curves of the ED-based algorithm for PUEA and jamming attack detection. Moreover, Tables 11.4 and 11.5 also show that the values of AUROC of the proposed algorithms are higher compared to the AUROC values of the ED-based algorithms to detect different hypothesis presented in (11.4). For example, the proposed algorithm outperforms the ED-based algorithm by 2.24 % in the case of PUEA and 6.88 % in case of jamming attack detection in terms of AUROC values. This is because the energy patterns in the residual and gradient vector enhance the detection capability of the proposed algorithm compared to the ED-based algorithm.

From an ML point-of-view, a trained model (classifier in this work) should not memorize the inputs used in its training. To investigate this quality in the trained ML classifier model in the proposed algorithm, Fig. 11.6 shows the training and testing losses versus epochs for the PUEA detection when $M = 100$. In view of this figure, it is evident that the accuracy of the training sets converges to the test set. These results signify the absence of overfitting, thereby validating the generalizability of the proposed model. In other words, the trained model does not memorize the training data. Here, it should be noted that we include the loss graph only for $M = 100$ case of PUEA to avoid repetition. For the other values of M and for the jammer case we observe the similar behavior in loss graphs.

11.6 Conclusions

In this paper, the convergence patterns of sparse recovery are exploited for the purpose of PUEA and jamming attack detection. Sparse recovery was conducted over a legitimate PU channel-dependent dictionary. Consequently, the signal from the legitimate node has smooth convergence as compared to the signal from the illegitimate node. Essentially, this awes to the fact that this signal is the only one compressible in the domain exclusively defined by this sparsifying dictionary. Besides, the non-compressive nature of a jamming signal with sparse coding over a PU channel-dependent dictionary was also exploited to detect jamming attacks. This detection algorithm made use of ML-based approaches. Numerical

experiments showed the effectiveness of the proposed algorithm and its superior performance compared to ED-based ML algorithms. These results were validated in terms of confusion matrices, ROC curves, and values of AUROC curves, as quality metrics. In terms of AUROC curve values, the proposed algorithm outperformed the ED-based algorithm by 2.24 % in the case of PUEA and 6.88 % in case of jamming attack detection.

Appendix Residual Energy Gradient Decay Analysis

The proposed algorithm is based on the convergence patterns in the sparse coding of the compressed received signal. More specifically, the proposed algorithm uses a channel-dependent dictionary to identify different characteristics of gradients and residuals to detect PUEA and jamming attack.

In this work, we employ the computationally-efficient OMP for sparse coding. Let us focus on its first iteration for the sake of simplicity. At the start of the first OMP iteration, the signal itself is used to initialize the zero-th residual $\boldsymbol{r}_0$. Afterwards, OMP chooses an atom ($\boldsymbol{d}$) from the atoms of the given dictionary $\boldsymbol{D_{PU}}$ that have the strongest similarity to the $\boldsymbol{r}_0$. This similarity is characterized by the projection corresponding to each atom as $\boldsymbol{E} = \boldsymbol{d}\boldsymbol{d}^{\dagger}$. The updated residual after the selection of atom can be given as

$$\boldsymbol{r}_1 = \boldsymbol{r}_0 - \boldsymbol{E}\boldsymbol{r}_0. \tag{11.5}$$

For simplicity, the least-squares refinement of OMP is ignored. With each iteration, the residual magnitude is decreasing and the pattern of the concatenated residual values ($\|\boldsymbol{r}_1\|_2^2$) is used for classification.

To this end, the first element in $\boldsymbol{G}$ can be represented as

$$\boldsymbol{G}(1) = \|\boldsymbol{r}_1\|_2^2 - \|\boldsymbol{r}_0\|_2^2 = \big\langle \boldsymbol{r_1}, \boldsymbol{r_1} \big\rangle - \big\langle \boldsymbol{r_0}, \boldsymbol{r_0} \big\rangle. \tag{11.6}$$

Using this gradient magnitude property we can differentiate the cases $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$, and $\mathcal{H}_3$. The general received signal can be given as: $\boldsymbol{y} = \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n}$ and we can write the $\boldsymbol{G}(1)$ as follows

$$\boldsymbol{G}(1) = \|\boldsymbol{y} - \boldsymbol{E}\boldsymbol{y}\|_2^2 - \|\boldsymbol{y}\|_2^2. \tag{11.7}$$

For the first hypothesis $\mathcal{H}_0$, $\boldsymbol{x} = 0$. Thus, $\boldsymbol{y}$ is merely noise and can be written as

$$\begin{aligned}\boldsymbol{G}(1)_{\mathcal{H}_0} &= \|\boldsymbol{n} - \boldsymbol{E}\boldsymbol{n}\|_2^2 - \|\boldsymbol{n}\|_2^2, \\ &= \big\langle \boldsymbol{n} - \boldsymbol{E}\boldsymbol{n}, \boldsymbol{n} - \boldsymbol{E}\boldsymbol{n} \big\rangle - \big\langle \boldsymbol{n}, \boldsymbol{n} \big\rangle, \\ &= \big\langle \boldsymbol{n}, \boldsymbol{n} \big\rangle - 2\big\langle \boldsymbol{n}, \boldsymbol{E}\boldsymbol{n} \big\rangle + \big\langle \boldsymbol{E}\boldsymbol{n}, \boldsymbol{E}\boldsymbol{n} \big\rangle - \big\langle \boldsymbol{n}, \boldsymbol{n} \big\rangle. \end{aligned} \tag{11.8}$$

With respect to the properties of projection, we know that $\big\langle \boldsymbol{E}\boldsymbol{n}, \boldsymbol{n} \big\rangle = \big\langle \boldsymbol{E}\boldsymbol{n}, \boldsymbol{E}\boldsymbol{n} \big\rangle = \|\boldsymbol{E}\boldsymbol{n}_2^2\|$. Hence, (11.8) can be written as

$$\boldsymbol{G}(1)_{\mathcal{H}_0} = -\|\boldsymbol{E}\boldsymbol{n}\|_2^2. \tag{11.9}$$

Following the same logic, $\boldsymbol{G}(1)$ for $\mathcal{H}_1$, $\mathcal{H}_2$ and $\mathcal{H}_3$ can be expressed as follows

$$\begin{aligned}\boldsymbol{G}(1) &= \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} - \boldsymbol{E}(\boldsymbol{h}\boldsymbol{x} + \boldsymbol{n}), \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} - \boldsymbol{E}(\boldsymbol{h}\boldsymbol{x} + \boldsymbol{n}) \big\rangle \\ &\quad - \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n}, \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} \big\rangle, \\ &= \boldsymbol{a} - 2\boldsymbol{b} + \boldsymbol{c} - \boldsymbol{d}, \end{aligned} \tag{11.10}$$

where $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ and $\boldsymbol{d}$ are defined next. Specifically, $\boldsymbol{a}$ can be written as

$$\begin{aligned}\boldsymbol{a} &= \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n}, \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} \big\rangle, \\ &= \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{h}\boldsymbol{x} \big\rangle + \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} \big\rangle + \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} \big\rangle + \big\langle \boldsymbol{n} + \boldsymbol{n} \big\rangle, \\ &= \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{h}\boldsymbol{x} \big\rangle + 2\big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} \big\rangle + \big\langle \boldsymbol{n} + \boldsymbol{n} \big\rangle. \end{aligned} \tag{11.11}$$

Assuming that the noise is independent of $\boldsymbol{h}\boldsymbol{x}$, $\big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n} \big\rangle = 0$, we can write (11.11) as

$$\boldsymbol{a} = \big\langle \boldsymbol{h}\boldsymbol{x} + \boldsymbol{h}\boldsymbol{x} \big\rangle + \big\langle \boldsymbol{n} + \boldsymbol{n} \big\rangle. \tag{11.12}$$

By its turn, $\boldsymbol{b}$ can be expressed as

$$\begin{aligned}\boldsymbol{b} &= \big\langle \boldsymbol{hx}+\boldsymbol{n}, \boldsymbol{E}(\boldsymbol{hx}+\boldsymbol{n})\big\rangle,\\ &= \big\langle \boldsymbol{hx}+\boldsymbol{n}, \boldsymbol{Ehx}+\boldsymbol{En}\big\rangle,\\ &= \big\langle \boldsymbol{hx}, \boldsymbol{Ehx}\big\rangle + \big\langle \boldsymbol{hx}, \boldsymbol{En}\big\rangle + \big\langle \boldsymbol{n}, \boldsymbol{Ehx}\big\rangle + \big\langle \boldsymbol{n}, \boldsymbol{En}\big\rangle,\\ &= \big\langle \boldsymbol{Ehx}, \boldsymbol{Ehx}\big\rangle + \big\langle \boldsymbol{hx}, \boldsymbol{En}\big\rangle + \big\langle \boldsymbol{n}, \boldsymbol{Ehx}\big\rangle + \big\langle \boldsymbol{En}, \boldsymbol{En}\big\rangle,\\ &= \big\langle \boldsymbol{Ehx}, \boldsymbol{Ehx}\big\rangle + \big\langle \boldsymbol{En}, \boldsymbol{En}\big\rangle, \end{aligned} \tag{11.13}$$

where $\big\langle \boldsymbol{hx}, \boldsymbol{En}\big\rangle = \big\langle \boldsymbol{n}, \boldsymbol{Ehx}\big\rangle = 0$.

Moreover, $\boldsymbol{c}$ can be expressed as

$$\begin{aligned}\boldsymbol{c} &= \big\langle \boldsymbol{E}(\boldsymbol{hx}+\boldsymbol{n}), \boldsymbol{E}(\boldsymbol{hx}+\boldsymbol{n})\big\rangle,\\ &= \big\langle \boldsymbol{Ehx}+\boldsymbol{En}, \boldsymbol{Ehx}+\boldsymbol{En}\big\rangle,\\ &= \big\langle \boldsymbol{Ehx}, \boldsymbol{Ehx}\big\rangle + \big\langle \boldsymbol{En}, \boldsymbol{En}\big\rangle. \end{aligned} \tag{11.14}$$

Lastly, $\boldsymbol{d}$ can be given as

$$\boldsymbol{d} = \big\langle \boldsymbol{hx}+\boldsymbol{hx}\big\rangle + \big\langle \boldsymbol{n}+\boldsymbol{n}\big\rangle = \boldsymbol{a}. \tag{11.15}$$

Based on (11.12), (11.13), (11.14) and (11.15), and making the appropriate substitution, $\boldsymbol{G}(1)$ can be written as

$$\begin{aligned}\boldsymbol{G}(1) &= \boldsymbol{a} - 2\boldsymbol{b} + \boldsymbol{c} - \boldsymbol{d},\\ &= -2\big\langle \boldsymbol{Ehx}, \boldsymbol{Ehx}\big\rangle - 2\big\langle \boldsymbol{En}, \boldsymbol{En}\big\rangle\\ &\qquad + \big\langle \boldsymbol{Ehx}, \boldsymbol{Ehx}\big\rangle + \big\langle \boldsymbol{En}, \boldsymbol{En}\big\rangle,\\ &= -\big\langle \boldsymbol{Ehx}, \boldsymbol{Ehx}\big\rangle - \big\langle \boldsymbol{En}, \boldsymbol{En}\big\rangle. \end{aligned} \tag{11.16}$$

Finally, the generic expression of the gradient magnitude for hypotheses $\mathcal{H}_1$, $\mathcal{H}_2$ and $\mathcal{H}_3$ can be expressed

$$\boldsymbol{G}(1)_{\mathcal{H}_1,\mathcal{H}_2,\mathcal{H}_3} = -\|\boldsymbol{Ehx}\|_2 - \|\boldsymbol{En}\|_2, \tag{11.17}$$

where $\boldsymbol{h}$ corresponds to $\boldsymbol{h}_{PU}$ in case of PU or $\boldsymbol{h}_i$ in case of PUE/jammer as explained in (11.4). Moreover, $\boldsymbol{x}$ will be structured in case of PU and PUE, while unstructured in the case of a jamming attack.

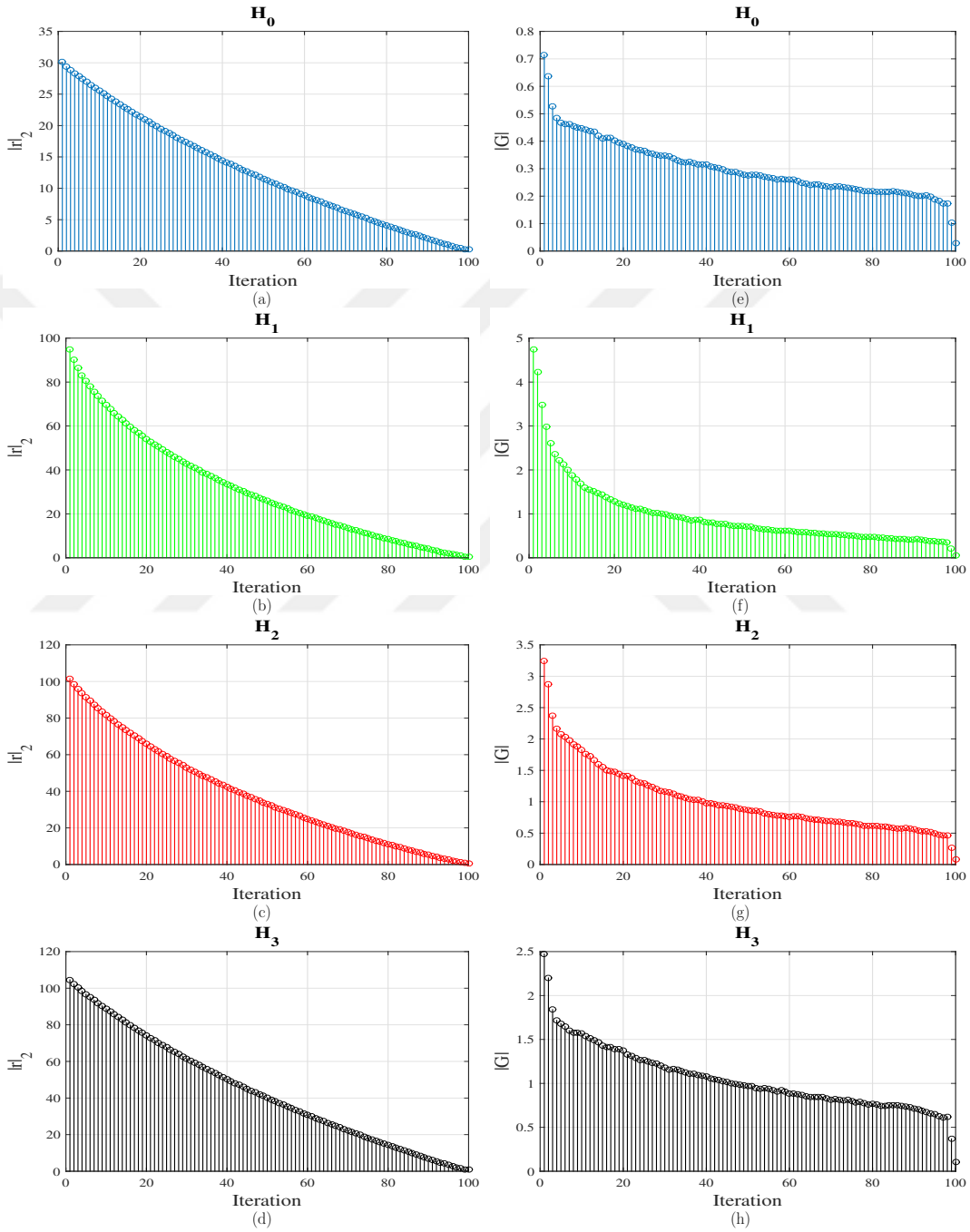


Fig. 11.2: The averages of $\|\boldsymbol{r}\|_2$ versus sparse coding iteration for received signals under hypotheses $\mathcal{H}_0$, $\mathcal{H}_1$, $\mathcal{H}_2$ and $\mathcal{H}_3$ are in (a), (b), (c), and (d), respectively, while the averages of $|\boldsymbol{G}|$ versus sparse coding iteration are presented in (e), (f), (g), and (h), respectively.

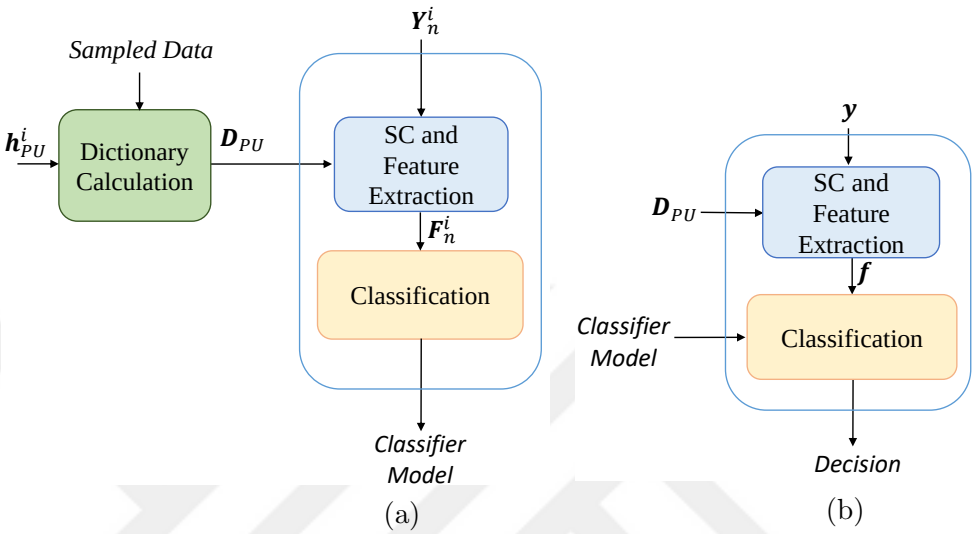


Fig. 11.3: An illustration of the proposed algorithm for (a) training stage, (b) testing stage.

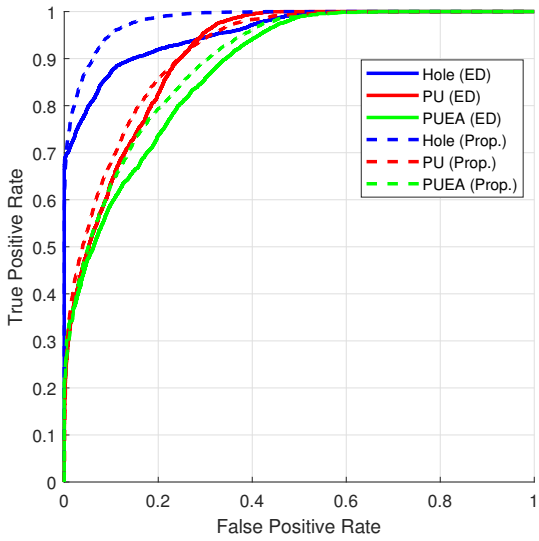


Fig. 11.4: Comparison of the proposed algorithm with the ED-based ML algorithm for PUEA detection using ROC curves.

Table 11.2: Confusion matrices for PUEA detection.

M=30								
0 dB			**5 dB**			**10 dB**		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
18.2	31.5	50.3	98.4	1.6	0.0	100.0	0.0	0.0
2.5	44.4	53.1	2.6	61.1	36.3	7.0	63.5	29.5
32.6	26.8	40.6	0.6	50.4	49.0	3.4	43.1	53.5
M=50								
0 dB			**5 dB**			**10 dB**		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
36.0	29.4	34.6	99.4	0.6	0.0	100.0	0.0	0.0
1.4	37.4	61.2	2.9	71.2	25.9	7.2	71.6	21.2
35.4	16.3	48.3	0.3	52.8	46.9	5.9	45.3	48.8
M=70								
0 dB			**5 dB**			**10 dB**		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
57.6	19.1	23.3	99.9	0.1	0.0	100.0	0.0	0.0
1.5	70.9	27.6	4.3	57.0	38.7	8.1	69.2	22.7
33.8	15.9	50.3	0.4	43.8	55.8	10.7	34.9	54.4
M=100								
0 dB			**5 dB**			**10 dB**		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
88.9	6.4	4.7	100.0	0.0	0.0	100.0	0.0	0.0
1.4	81.2	17.4	1.0	53.0	46.0	4.0	79.4	16.6
32.2	6.7	61.1	0.3	17.0	82.7	3.2	35.0	61.8

Table 11.3: Confusion matrices for jamming attack detection.

M=30								
0 dB			5 dB			10 dB		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
12.5	25	62.5	98.4	1.6	0	100	0	0
0.9	44.6	54.5	2.3	54.8	42.9	3.5	58	38.5
27.3	25.6	47.1	0	27.9	72.1	1.3	26.2	72.5
M=50								
0 dB			5 dB			10 dB		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
24.5	20.9	54.6	99.5	0.5	0	100	0	0
0.9	51.9	47.2	2.4	65.3	32.3	4.6	69.7	25.7
42.7	14.5	42.8	0	23.5	76.5	2.6	20	77.4
M=70								
0 dB			5 dB			10 dB		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
29.8	15	55.2	99.5	0.5	0	100	0	0
0.2	63.3	36.5	2.1	65.6	32.3	4.3	74.1	21.6
37.6	14.3	48.1	0	18.7	81.3	2.6	16.4	81
M=100								
0 dB			5 dB			10 dB		
$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$	$\mathcal{H}_0$	$\mathcal{H}_1$	$\mathcal{H}_2$
58.2	3	38.8	100	0	0	100	0	0
0.3	90.6	9.1	0.7	88.8	10.5	1.1	93.8	5.1
37	3.7	59.3	0	10.7	89.3	0.2	4.9	94.9

Table 11.4: AUROC values for PUEA.

	PU	**Hole**	**PUE**
ED-based	0.9089	0.9560	0.8719
Proposed	0.9152	0.9828	0.8943

Table 11.5: AUROC values for jamming attack.

	PU	**Hole**	**Jammer**
ED-based	0.9097	0.9542	0.8820
Proposed	0.9830	0.9637	0.9508

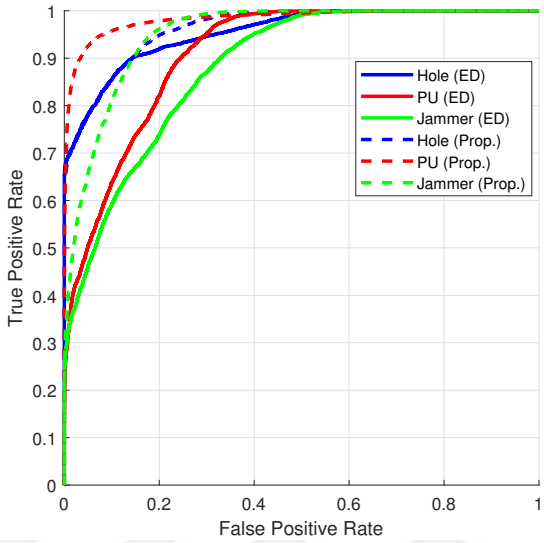


Fig. 11.5: Comparison of the proposed algorithm with the ED-based ML algorithm for jamming attack detection using ROC curves.

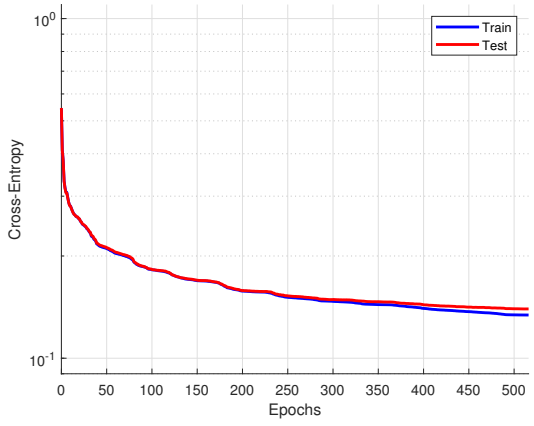


Fig. 11.6: Model loss graph for the PUEA detection when $M = 100$.

Chapter 12

Conclusion and Recommendations

12.1 Concluding Remarks

To deal with the challenge of secure communication for future wireless communication; novel physical layer security solutions are proposed and developed in this thesis. The conclusions drawn from different research studies can be summarized as follows:

- The generation of secret keys from reciprocal wireless channel by exploiting their randomness nature, is an emerging area of interest to provide secure communication. One of the main challenges in this domain is to increase the secret key length, extracted from the shared channel coefficients between two legitimate communication parties, while maintaining its randomness and uniformity. This paper has provided a secret key generation method, called channel quantization with singular value decomposition (CQSVD), which exploits the reciprocity of $M \times M$ MIMO channel. In this method, a phase randomization (PR) key vector for symbol level encryption is generated by applying alternative form of SVD on channel's phase and magnitude

matrices. It was shown that for $M \times M$ MIMO channel, a key length of $(2M^3)$ can be generated. Simulations with a simple 4×4 MIMO channel have been presented. The scheme has been analyzed for perfect and imperfect channel estimation as well as for perfect and imperfect channel reciprocity.

- In indices based work, efficient algorithms are proposed for secret key generation from the wireless channel, where key bits are not only generated by amplitudes of the subcarriers but also by the indices of subcarriers corresponding to highest channel gains. Specifically, in the first step, the communicating nodes convert the correlated frequency response of the channel at them into random order by exploiting random interleaver. Afterwards, the estimated channel response in the frequency domain at them is partitioned into small subblocks. Finally, the key bits are generated by both amplitudes of individual subcarriers by comparing with their mean as well as by indices/positions of good sub-channels in each subblock by employing a look-up table. The proposed novel dimensions for secret key generation results in the enhancement of overall KGR without degrading overall performance as shown by simulation results. More specifically, there is a 50 % increase in key rate as shown by JKG performance compared to the CKG approach due to the involvement of the proposed dimensions of key generation. For future work, different variations of the proposed algorithm assuming different activation ratios and block sizes can be considered. In addition, the proposed algorithm of secret key generation can be extended to other domains such as time, space, and code domains.

- Channel shortening based work presents a simple, spectral and power efficient scheme for providing secure OFDM communication system. In this work, a practical spectral and power efficient security method is presented that is based on channel shortening. Channel shortening equalizer coefficients are designed based on Bob's channel and CS is used at transmitter in such a way that the effective channel ensures no ISI at Bob, while causing ISI and performance degradation at Eve, thus, QoS based security can be provided. The simulation results are given for both perfect and imperfect

channel estimation to demonstrate the effectiveness and robustness of the proposed algorithm. The proposed scheme can provide QoS based security and can successfully secure voice communication between legitimate parties. The idea can be extended to provide security to any single carrier or multi carrier CP based system.

- In OFDM-IM based work, effective algorithms that change SAR and/or CM adaptively in each subblock of the OFDM-IM scheme based on the channel characteristics of the legitimate receiver are proposed for enhancing PLS and SE. Particularly, the first two algorithms named as OFDM-AIM-FCM and OFDM-AIM-ACM are designed for enhancing PLS and SE, while the third algorithm named as OFDM-VIM-VCM is designed for QoS based communication for enhancing SE. Simulation results show that the first two algorithms can provide significant security enhancement whereas the third algorithm ensures QoS based communication aiming to maximize spectral efficiency.

- An effective technique for reliable and secure communication is presented for IoT devices. Channel-dependent pre-coders with dual-transmission approach are jointly exploited to ensure a reliable as well as secure communication against internal and external eavesdropping. More specifically, users' pre-coded data is superimposed in the first step. Afterward, the mixture is sent in two transmissions in such a way that after combining signals from the first and the second transmissions, the legitimate receivers will get the reliable signal without complex processing while the external eavesdropper will get the degraded version of the signal. Moreover, the proposed algorithm also ensures that the users are also not able to eavesdropper each other's data. Simulation results proved that the proposed algorithm can ensure secure communication and suitable for IoT-based devices because it does not require complex processing at the receivers. For future work, the extension of the proposed algorithm for active eavesdropper case will be considered.

- In this work, a reliable and power efficient security technique for an untrusted DAF based cooperative communication is proposed.The technique

enables us to keep utilizing the benefits provided by DAF relay, while keeping information secure from it. The proposed technique is more power efficient as it does not require continuous power for jamming signal. The simulation results are provided to demonstrate the effectiveness of the proposed algorithm for both perfect and imperfect channel estimation cases. Future studies can examine untrusted-relay-assisted D2D based heterogeneous networks and untrusted secondary users in cognitive communication.

- In this work, a cooperative game theory, based on NBS, is applied to develop a fair user association scheme to enhance the physical layer security of downlink hetnets. Firstly, a bargaining scheme for two BSs is presented. And, then scheme for two BSs is extended to multi-player bargaining scheme. In the multi player bargaining scheme, firstly, the BSs are grouped in to pairs by Hungarian algorithm and then in each pair two player bargaining scheme is applied. The two BSs case have complexity of $O(N \log_2 N)$ while multi player case have complexity of $O(M^2 N \log_2 N + M^3)$. Simulation results indicate that the proposed solution can enhance security while providing fairness among users.

- The majority of the PLS research focused on the single attack but neglected the consideration of joint attacks in wireless networks, such as joint attacks of eavesdropping, spoofing, and jamming. In cognitive security work, a new, yet promising research direction to defend against joint attacks is presented. We proposed an entirely novel concept related to intelligent security with the aims of providing proactive, adaptive, reliable, and robust security solutions for wireless communication systems. The cognitive security engine is driven by the information it receives from the upper layers and PHY. This information is then processed by the system to first determine the best suited level of security for the particular use case and scenario. Afterward, appropriate resources are allocated to ensure secure communication.

- NOMA promises high spectral efficiency, low latency, and massive connectivity, while PLS offers simple and effective security solutions. Together, these two technologies are capable of supporting the exceeding efficiency and security requirements of 5G and beyond networks. In this article, the

key security design requirements of NOMA and the strength of PLS as a solution to fulfill these requirements are discussed. By employing PLS to NOMA, spectrally efficient, adaptive, and secure systems can be realized. However, the challenges and future recommendations explained in this work need to be investigated further to address the open issues. Practical secure NOMA systems can be developed by modification of current PLS techniques and/or proposing new novel techniques that do not require extra processing, extra signaling, or major modification in the receiver structure.

- In this paper, the convergence patterns of sparse recovery are exploited for the purpose of PUEA and jamming attack detection. Sparse recovery was conducted over a legitimate PU channel-dependent dictionary. Consequently, the signal from the legitimate node has smooth convergence as compared to the signal from the illegitimate node. Essentially, this awes to the fact that this signal is the only one compressible in the domain exclusively defined by this sparsifying dictionary. Besides, the non-compressive nature of a jamming signal with sparse coding over a PU channel-dependent dictionary was also exploited to detect jamming attacks. This detection algorithm made use of ML-based approaches. Numerical experiments showed the effectiveness of the proposed algorithm and its superior performance compared to ED-based ML algorithms. These results were validated in terms of confusion matrices, ROC curves, and values of AUROC curves, as quality metrics. In terms of AUROC curve values, the proposed algorithm outperformed the ED-based algorithm by 2.24 % in the case of PUEA and 6.88 % in case of jamming attack detection.

12.2 Challenges and Future Research Directions

This section presents the challenges and future research directions for designing practical, efficient, and secure future wireless systems.

- Secrecy design based on service requirements From key-based Shannon's model to key-lessWyner's mode, much of the PLS techniques are designed to simply obtain secure messaging service without focusing on the security level needed by other applications such as URLLC, video, voice, gaming, streaming, and mMTC. For such applications, the primary objective is to offer a reliable data transfer to the user, which lies within the standard QoS requirements. Under these conditions, it can be inferred that the perfect secrecy, such that there is no data leakage to Eve, is not a strict requirement for providing a secure service. The truth is that the QoS requirements of every service are different from the others, and if Eve is operating below these requirements, practical service-based secrecy can be attained. Consequently, redesigning the present PLS schemes from a realistic point of view, which takes into consideration the QoS requirements of different services, can direct future research in this domain.

- Cross-layer security design Although the cross-layer security design is a modern and promising research area yet it does not have the attention it deserves. This domain of security includes cross APPPLS, cross NET-PLS, cross MAC-PLS, and their hybrid designs. These relatively new approaches include the functionalities, principles, and mechanisms of upper layers in the PLS design process and integrating them jointly to enhance the security performance.

- PAPR of AN-based and precoding security techniques The PAPR is linked with the nonlinearities in power amplifiers. However, within the realms of PLS and its literature, the influence of the precoding and AN-based security techniques on PAPR is often forgotten. A lack of tangible work on this practically crucial aspect might even hinder the application of many effective AN-based security techniques in real-world situations. Hence, considering such issues while designing security schemes is strongly recommended.

- Security in LOS environment Ensuring secure communication in LOS scenarios is quite challenging if the eavesdropper is located within the same

direction as that of Bob. Under such circumstances, many PLS techniques, including conventional beamforming, directional modulation, AN-based MIMO techniques, etc., will not be able to ensure secure communication. In general, designing practical PLS approaches that can retain their applicability in diverse scenarios, including time-invariant and nondispersive channels, has become increasingly important. Additionally, it is assumed in the majority of PLS techniques Physical layer security designs for 5G and beyond 581 that Bob's channel is uncorrelated with respect to Eve's channel. However, this might not always be the case, for example, in poor scattering environment, there may be a strong correlation between Bob's and Eve's channels. Under such circumstances, the level of PLS will reduce significantly. Therefore, investigating and reviewing the present PLS techniques under these conditions open new doors to the applications of the security methods available currently.

- Robust channel estimation and channel reciprocity calibration The majority of the PLS techniques (against eavesdropping and authentication) revolve around exploiting the CSI and its availability at the transmitter and receiver sides. As a result, it is imperative to perform robust channel estimations and reciprocity calibration, which is undoubtedly a challenging task to achieve in practice. Hence, the effect of channel estimation error and reciprocity mismatch should be considered while designing any security algorithm to ensure that it is robust against all the aforementioned drawbacks. The issue can be solved by incorporating efficient practical channel calibration and estimation methods in the design process.

- Joint design of secrecy, throughput, delay, and reliability An interesting dimension that is of great importance but has not been explored with interest in recent times in the literature is the combined design of secrecy, throughput, delay, reliability, and the trade-off among them. Generally, offering PHY-secrecy constraints may unwittingly compromise other system requirements. AN-based techniques, for instance, impact power efficiency, whereas channel coding-based techniques prove to be detrimental to spectral efficiency. Therefore, it is imperative to include design principles that

directly affect the system performance criteria such as delay, packet loss, throughput, and PER in the future research work surrounding security.

- Impersonation attacks PHY-authentication mostly depends on the uniqueness of CSI andAFE imperfections of any transmitter or receiver. However, PHY-authentication is also vulnerable to impersonation attacks in the case when an attacker is near to a legitimate device. Moreover, preprocessing of the transmitted signal can alter the channel estimation at the receiver. Furthermore, counterfeiting attacks can also be launched on AFE-based authentication. Protecting PHY-authentication from impersonation attacks is still an open area for further research.

- Challenges related to solution against jamming attacks Designing practical generic jamming detection methods and countermeasures that can deal with multiple jamming attacks in different types of wireless networks is still an open issue. The majority of jamming detection and anti-jamming solutions are focused on the static environment. The design of effective solutions in the case of a mobile network environment, where different jammers can change their positions, is quite challenging. Moreover, the majority of the solutions are not efficient in terms of resources, and there is an urgent need for designing novel and resource-efficient solutions. Furthermore, there is also a need for designing intelligent anti-jammers that can differentiate whether the packet is lost due to jamming or weak channel.

- Mixed attacks in wireless networks and cognitive security

  The majority of the PLS research focused on the single attack but neglected the consideration of joint attacks in wireless networks, such as joint attacks of eavesdropping, spoofing, and jamming. A new, yet promising research direction to defend against joint attacks is presented in [49,50]. The authors proposed an entirely novel concept related to intelligent security, called, cognitive security, for wireless communication, with the aims of providing proactive, adaptive, reliable, and robust security solutions for wireless communication systems. The conceptual block diagram of the framework is shown in Figure 18.20. The cognitive security engine is driven by the information it receives from the upper layers and PHY. This information is then

processed by the system to first determine the best suited level of security for the particular use case and scenario. Afterward, appropriate resources are allocated to ensure secure communication.

- A new direction for PLS In the literature, PLS is considered as a solution to provide security against confidentiality, spoofing, and jamming. However, PLS is beyond that. PLS, in general, endorses the process of someone not being able to extract any useful information from the transmitted PHY-signals. The PHY-information includes power, location, angle, data, mobility, velocity, size, power, SINR, RF-front properties, impairments, fingerprinting, state, frequency, modulation, RSSI, and so on. In other words, the security concept is not only about protecting data and communication, but it also envisions safeguarding the whole radio environment map. Hence, PLS can secure all properties of PHY-signals so that these properties cannot be used by any illegitimate node for attacking the communication, impersonating, eavesdropping, tracking, or any other misuse. More specifically, even one cannot equalize, and demodulate but can still get some information about the PHY-properties in the earlier phase of the receiver. For example, radar can estimate the speed, location, size of an object without demodulating the signal. Hence, securing all PHY-properties of signals is necessary to ensure secure future wireless networks. This aspect of PLS needs to be considered for future communication systems.

- Hybrid security techniques It is worth mentioning that hybrid security techniques offer enhanced security on more than one level. Such approaches consist of multiple levels of security, where one stems from SINR-based techniques while the other is either from complexity-based techniques or conventional cryptography techniques.

  Logically, the combination of different schemes in a single approach makes the system more robust towards hacks and eavesdropping. However, it will also increase the complexity of the overall system.

  Combination of different techniques and their combined effect on security is an interesting area for future research.

Bibliography

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

[2] 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*, pp. 6190–6204, Nov. 2018.

[3] X.-Q. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-enhancing scheme for spatial modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2017.

[4] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE J. Sel. Areas Commun.*, vol. 36, pp. 788–801, April 2018.

[5] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multi-cast uni-cast streaming," *IEEE Trans. Commun.*, vol. 65, pp. 3151–3163, July 2017.

[6] 3rd Generation Partnership Project (3GPP), "Policy and charging control architecture," Technical Report TS 23.203 V11.6.0, 2012.

[7] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 18, pp. 1617–1655, Feb. 2016.

[8] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?," *IEEE J. Sel. Areas Commun.*, vol. 32, pp. 1065–1082, June 2014.

[9] M. F. Khan, F. A. Bhatti, A. Habib, S. Jangsher, M. I. Khan, I. Zafar, S. M. Shah, M. A. Jamshed, and J. Iqbal, "Analysis of macro user offloading to femto cells for 5G cellular networks," in *Int. Symposium on Wireless Systems and Networks (ISWSN)*, pp. 1–6, Nov 2017.

[10] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, pp. 1–14, December 2017.

[11] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, pp. 1–1, 2018.

[12] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 21, pp. 1773–1828, Oct. 2019.

[13] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[14] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[15] H. M. Furqan, J. Hamamreh, H. Arslan, *et al.*, "Physical layer security for noma: Requirements, merits, challenges, and recommendations," *arXiv preprint arXiv:1905.05064*, May 2019.

[16] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, pp. 679–695, April 2018.

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

[18] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *International Symposium on Wireless Communication Systems (ISWCS)*, (Poznań, Poland), pp. 597–602, IEEE, Sep 2016.

[19] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, pp. 2933–2945, Aug. 2007.

[20] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, pp. 6428–6443, Oct. 2011.

[21] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Transactions on Information Theory*, vol. 56, pp. 2307–2359, May 2010.

[22] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of ofdm systems using channel shortening," in *IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, (Montreal, Canada), pp. 1–5, Oct 2017.

[23] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Adaptive ofdm-im for enhancing physical layer security and spectral efficiency of future wireless networks," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[24] 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, Nov. 2017.

[25] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Transactions on Signal Processing*, vol. 59, pp. 351–361, Sep. 2011.

[26] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Transactions on Wireless Communications*, vol. 17, pp. 563–573, Jan. 2018.

[27] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *IEEE International Conference on Communications (ICC)*, (Cape Town, South Africa), pp. 1–5, May. 2010.

[28] H. M. Wang, M. Luo, X. G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Processing Letters*, vol. 20, pp. 39–42, Nov. 2013.

[29] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Energy-efficient secrecy in wireless networks based on random jamming," *IEEE Transactions on Communications*, vol. 65, pp. 2522–2533, June 2017.

[30] 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 Transactions on Wireless Communications*, vol. 12, pp. 2717–2729, June 2013.

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

[32] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180–2189, June 2008.

[33] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform gaussian signaling," in *IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–6, Nov. 2009.

[34] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *IEEE Global Telecommunications Conference (GLOBECOM)*, (New Orleans, USA), pp. 1–5, Dec. 2008.

[35] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Communications Magazine*, vol. 53, pp. 33–39, June 2015.

[36] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom, (New York, NY, USA), pp. 128–139, ACM, Sep. 2008.

[37] Y. Abdallah, M. Abdel Latif, M. Youssef, A. Sultan, and H. El Gamal, "Keys through ARQ: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 737–751, Sep. 2011.

[38] S. Naderi, D. B. da Costa, and H. Arslan, "Joint random subcarrier selection and channel-based artificial signal design aided pls," *IEEE Wireless Communications Letters*, pp. 1–1, 2020.

[39] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Transactions on Communications*, vol. 64, pp. 2578–2588, June 2016.

[40] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proceedings of the 29th Conference on Information Communications*, (San diego, USA), pp. 1–9, May 2010.

[41] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secure communication via untrusted switchable decode-and-forward relay," in *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, (Valencia, Spain), pp. 1333–1337, June 2017.

[42] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 1666–1674, Oct. 2012.

[43] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 1578–1588, August 2012.

[44] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, pp. 56–62, Oct. 2010.

[45] C. Pei, N. Zhang, X. S. Shen, and J. W. Mark, "Channel-based physical layer authentication," in *2014 IEEE Global Communications Conference (GLOBECOM)*, (Texas, USA), pp. 4114–4119, IEEE, Dec. 2014.

[46] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 14–24, Feb. 2012.

[47] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, pp. 41–47, May 2006.

[48] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "Spread: Foiling smart jammers using multi-layer agility," in *IEEE International Conference on Computer Communications (INFOCOM)*, (Barcelona, Spain), pp. 2536–2540, May 2007.

[49] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, Oct 1949.

[50] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, pp. 1550–1573, Third 2014.

[51] and and and, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *2012 Proceedings IEEE INFOCOM*, pp. 927–935, March 2012.

[52] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, (New York, NY, USA), pp. 401–410, ACM, 2007.

[53] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom '08, (New York, NY, USA), pp. 128–139, ACM, 2008.

[54] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, May 1993.

[55] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, pp. 1121–1132, July 1993.

[56] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. ii. cr capacity," *IEEE Transactions on Information Theory*, vol. 44, pp. 225–240, Jan 1998.

[57] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels .i. definitions and a completeness result," *IEEE Transactions on Information Theory*, vol. 49, pp. 822–831, April 2003.

[58] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part ii: the simulatability condition," *IEEE Transactions on Information Theory*, vol. 49, pp. 832–838, April 2003.

[59] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels .iii. privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, pp. 839–851, April 2003.

[60] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Communications Letters*, vol. 4, pp. 52–55, Feb 2000.

[61] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, pp. 2593–2597, IEEE, 2006.

[62] C. Ye, A. Reznik, G. Sternburg, and Y. Shah, "On the secrecy capabilities of itu channels," in *2007 IEEE 66th Vehicular Technology Conference*, pp. 2030–2034, IEEE, 2007.

[63] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *arXiv preprint arXiv:0910.5027*, 2009.

[64] T. Shimizu, H. Iwai, and H. Sasaoka, "Reliability-based sliced error correction in secret key agreement from fading channel," in *2010 IEEE Wireless Communication and Networking Conference*, pp. 1–6, IEEE, 2010.

[65] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 3013–3016, IEEE, 2008.

[66] Y. Liu, S. C. Draper, and A. M. Sayeed, "Secret key generation through ofdm multipath channel," in *2011 45th Annual Conference on Information Sciences and Systems*, pp. 1–6, IEEE, 2011.

[67] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1484–1497, Oct 2012.

[68] Y. E. H. Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," in *2011 Wireless Telecommunications Symposium (WTS)*, pp. 1–6, IEEE, 2011.

[69] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *2011 Proceedings IEEE INFOCOM*, pp. 1422–1430, April 2011.

[70] F. Renna, M. R. Bloch, and N. Laurenti, "Semi-blind key-agreement over mimo fading channels," *IEEE Transactions on Communications*, vol. 61, pp. 620–627, February 2013.

[71] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 381–392, Sep. 2010.

[72] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated mimo channels," in *2013 IEEE Globecom Workshops (GC Wkshps)*, pp. 1245–1250, Dec 2013.

[73] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, March 2010.

[74] C. Wu, P. Lan, P. Yeh, C. Lee, and C. Cheng, "Practical physical layer security schemes for mimo-ofdm systems using precoding matrix indices," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 1687–1700, Sep. 2013.

[75] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Phys. Rev. E*, vol. 69, p. 066138, Jun 2004.

[76] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM wireless communications with MATLAB*. John Wiley & Sons, 2010.

[77] J. W. Demmel, *Applied Numerical Linear Algebra*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 1997.

[78] MATLAB and S. T. Release, "The mathworks, inc," 2016.

[79] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 205–215, Feb 2011.

[80] 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 Conference, pp. 1–6, April 2016.

[81] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, 2019.

[82] 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.

[83] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE INFOCOM*, pp. 3048–3056, April 2013.

[84] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 5, pp. 1484–1497, 2012.

[85] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, pp. 1422–1430, Apr 2011.

[86] 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.

[87] 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.

[88] T. Mao, Q. Wang, Z. Wang, and S. Chen, "Novel index modulation techniques: A survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 315–348, 2019.

[89] J. M. Hamamreh, "Improving the physical layer security of IoT-5G systems," in *Artificial Intelligence in IoT*, pp. 25–44, Springer, 2019.

[90] Y. Cho, J. Kim, W. Yang, and C. Kang, *MIMO-OFDM Wireless Communication with MATLAB*. Singapore: Wiley, Nov. 2010.

[91] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE INFOCOM*, pp. 3048–3056, 2013.

[92] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *2016 International Symposium on Wireless Communication Systems (ISWCS)*, pp. 597–602, 2016.

[93] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1191–1194, 2017.

[94] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., Booz-allen and hamilton inc mclean va, 2001.

[95] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Secure key generation from ofdm subcarriers' channel responses," in *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 1302–1307, IEEE, 2014.

[96] H. Li, X. Wang, and J. Chouinard, "Eavesdropping-resilient ofdm system using sorted subcarrier interleaving," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 1155–1165, Feb 2015.

[97] H. Qin, Y. Sun, T. Chang, X. Chen, C. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap ofdm with discrete inputs," *IEEE Transactions on Wireless Communications*, vol. 12, pp. 2717–2729, June 2013.

[98] 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, IEEE, 2014.

[99] P. J. W. Melsa, R. C. Younce, and C. E. Rohrs, "Impulse response shortening for discrete multitone transceivers," *IEEE Transactions on Communications*, vol. 44, pp. 1662–1672, Dec 1996.

[100] J. S. Chow and J. M. Cioffi, "A cost-effective maximum likelihood receiver for multicarrier systems," in *[Conference Record] SUPERCOMM/ICC '92 Discovering a New World of Communications*, pp. 948–952 vol.2, June 1992.

[101] S. Celebi, "Interblock interference (ibi) minimizing time-domain equalizer (teq) for ofdm," *IEEE Signal Processing Letters*, vol. 10, pp. 232–234, Aug 2003.

[102] P. Zhang and J. Qin, "A simple channel shortening equalizer for wireless tdd-ofdm systems," in *2010 IEEE International Conference on Wireless Communications, Networking and Information Security*, pp. 83–86, IEEE, 2010.

[103] N. Al-Dhahir and J. M. Cioffi, "Optimum finite-length equalization for multicarrier transceivers," *IEEE Transactions on Communications*, vol. 44, pp. 56–64, Jan 1996.

[104] G. Arslan, B. L. Evans, and S. Kiaei, "Equalization for discrete multitone transceivers to maximize bit rate," *IEEE Transactions on Signal Processing*, vol. 49, pp. 3123–3135, Dec 2001.

[105] K. Vanbleu, G. Ysebaert, G. Cuypers, M. Moonen, and K. Van Acker, "Bitrate-maximizing time-domain equalizer design for dmt-based systems," *IEEE Transactions on Communications*, vol. 52, pp. 871–876, June 2004.

[106] R. K. Martin, J. Balakrishnan, W. A. Sethares, and C. R. Johnson, "A blind adaptive teq for multicarrier systems," *IEEE Signal Processing Letters*, vol. 9, pp. 341–343, Nov 2002.

[107] 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 Conference*, pp. 1–7, IEEE, 2016.

[108] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secure communication via untrusted switchable decode-and-forward relay," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1333–1337, IEEE, 2017.

[109] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for ofdm systems along with hardware implementation," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1338–1343, June 2017.

[110] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with svd for reciprocal mimo channels," in *2016 International Symposium on Wireless Communication Systems (ISWCS)*, pp. 597–602, Sep. 2016.

[111] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[112] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2016.

[113] E. Basar, M. Wen, R. Mesleh, M. Di Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE Access*, vol. 5, pp. 16693–16746, 2017.

[114] E. Basar, "Multiple input multiple output orthogonal frequency division multiplexing with index modulation, mimo-ofdm-im, communications system," May 1 2018. US Patent 9,960,831.

[115] J. Choi, "Coded ofdm-im with transmit diversity," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 3164–3171, 2017.

[116] J. Li, M. Wen, X. Cheng, Y. Yan, S. Song, and M. H. Lee, "Generalized precoding-aided quadrature spatial modulation," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1881–1886, 2016.

[117] M. Wen, E. Basar, Q. Li, B. Zheng, and M. Zhang, "Multiple-mode orthogonal frequency division multiplexing with index modulation," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3892–3906, 2017.

[118] E. Soujeri, G. Kaddoum, M. Au, and M. Herceg, "Frequency index modulation for low complexity low energy communication networks," *IEEE Access*, vol. 5, pp. 23276–23287, 2017.

[119] M. Au, G. Kaddoum, F. Gagnon, and E. Soujeri, "A joint code-frequency index modulation for low-complexity, high spectral and energy efficiency communications," *arXiv preprint arXiv:1712.07951*, 2017.

[120] E. Soujeri, G. Kaddoum, and M. Herceg, "Design of an initial condition-index chaos shift keying modulation," *Electronics Letters*, vol. 54, no. 7, pp. 447–449, 2018.

[121] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *2011 Proceedings IEEE INFOCOM*, pp. 1422–1430, April 2011.

[122] 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 Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2717–2729, 2013.

[123] 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.

[124] 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 Conference*, pp. 1–7, April 2016.

[125] E. Güvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *2014 IEEE International Conference on Communications Workshops (ICC)*, pp. 813–818, June 2014.

[126] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure ofdma systems," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 6, pp. 2572–2585, 2012.

[127] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of ofdm systems using channel shortening," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–5, Oct 2017.

[128] 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.

[129] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, 2015.

[130] Y. Lee, H. Jo, Y. Ko, and J. Choi, "Secure index and data symbol modulation for ofdm-im," *IEEE access*, vol. 5, pp. 24959–24974, 2017.

[131] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1351–1354, 2015.

[132] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *2016 8th International Conference on Wireless Communications Signal Processing (WCSP)*, pp. 1–5, Oct 2016.

[133] X.-Q. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-enhancing scheme for spatial modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2017.

[134] P. Robertson, E. Villebrun, and P. Hoeher, "A comparison of optimal and sub-optimal map decoding algorithms operating in the log domain," in *Proceedings IEEE International Conference on Communications ICC'95*, vol. 2, pp. 1009–1013, IEEE, 1995.

[135] H. Jafarkhani, *Space-time coding: theory and practice*. Cambridge university press, 2005.

[136] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.

[137] H. Li, X. Wang, and J.-Y. Chouinard, "Eavesdropping-resilient ofdm system using sorted subcarrier interleaving," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 1155–1165, 2014.

[138] 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.

[139] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Physical Communication*, vol. 25, pp. 14–25, 2017.

[140] J. Faezah and K. Sabira, "Adaptive modulation for ofdm systems," *International journal of communication networks and information security*, vol. 1, no. 2, p. 1, 2009.

[141] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (otdm) waveform for 5g and beyond," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1191–1194, 2017.

[142] F. Wu, R. Zhang, L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 467–471, 2016.

[143] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–5, IEEE, 2016.

[144] X. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-enhancing scheme for spatial modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2018.

[145] H. M. Furqan, M. A. Aygul, M. Nazzal, and H. Arslan, "Primary User Emulation and Jamming Attack Detection in Cognitive Radio via Sparse Coding," *arXiv e-prints*, p. arXiv:2006.09231, June 2020.

[146] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[147] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *IEEE 28th Annual Int. Symposium on Personal, Indoor, and Mobile Radio Commun. (PIMRC)*, pp. 1–5, Oct 2017.

[148] 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.

[149] 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, no. 6, pp. 2717–2729, 2013.

[150] Z. Feng, *Security, Reliability and Performance Issues in Wireless Networks*. PhD thesis, USA, 2013. AAI3559975.

[151] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, pp. 1451–1458, Oct 1998.

[152] L. Hanzo, L.-L. Yang, E. Kuan, and K. Yen, *Single-and multi-carrier DS-CDMA: multi-user detection, space-time spreading, synchronisation, standards and networking*. John Wiley & Sons, 2003.

[153] K. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative communications and networking*. Cambridge university press, 2009.

[154] B. Can, H. Yomo, and E. De Carvalho, "Hybrid forwarding scheme for cooperative relaying in ofdm based networks," in *2006 IEEE International Conference on Communications*, vol. 10, pp. 4520–4525, IEEE, 2006.

[155] M. Fadhil, M. Ismail, A. Saif, N. S. Othman, and M. Khaleel, "Cooperative communication system based on convolutional code cdma techniques," in *2014 IEEE REGION 10 SYMPOSIUM*, pp. 594–599, IEEE, 2014.

[156] Z. Si, R. Thobaben, and M. Skoglund, "Bilayer ldpc convolutional codes for decode-and-forward relaying," *IEEE transactions on communications*, vol. 61, no. 8, pp. 3086–3099, 2013.

[157] S. Rawat, *Implementation of a forward error correction technique using convolutional encoding with Viterbi decoding*. PhD thesis, Ohio University, 2004.

[158] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with svd for reciprocal mimo channels," in *2016 International Symposium on Wireless Communication Systems (ISWCS)*, pp. 597–602, IEEE, 2016.

[159] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (otdm) waveform for 5g and beyond," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1191–1194, 2017.

[160] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 650–660, 2011.

[161] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2011.

[162] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE wireless communications letters*, vol. 4, no. 1, pp. 46–49, 2014.

[163] A. H. Abd El-Malek, A. M. Salhab, and S. A. Zummo, "Optimal power allocation for enhancing physical layer security in opportunistic relay networks in the presence of co-channel interference," in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2015.

[164] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, pp. 1–5, IEEE, 2008.

[165] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 682–694, 2013.

[166] 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 Conference*, pp. 1–6, IEEE, 2016.

[167] 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 Conference*, pp. 1–7, IEEE, 2016.

[168] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 193–202, IEEE, 2007.

[169] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

[170] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping—part i: System design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70–79, 2012.

[171] X. Li, C. Yu, M. Hizlan, W.-T. Kim, and S. Park, "Physical layer watermarking of direct sequence spread spectrum signals," in *MILCOM 2013-2013 IEEE Military Communications Conference*, pp. 476–481, IEEE, 2013.

[172] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE vehicular technology conference*, vol. 62, p. 1906, Citeseer, 2005.

[173] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on selected areas in communications*, vol. 26, no. 1, pp. 25–37, 2008.

[174] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *International Conference on Wired/Wireless Internet Communications*, pp. 186–200, Springer, 2004.

[175] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[176] Mingbo Xiao, Xudong Wang, and Guangsong Yang, "Cross-layer design for the security of wireless sensor networks," in *2006 6th World Congress on Intelligent Control and Automation*, vol. 1, pp. 104–108, 2006.

[177] G. Thamilarasu and R. Sridhar, "Exploring cross-layer techniques for security: Challenges and opportunities in wireless networks," in *MILCOM 2007 - IEEE Military Communications Conference*, pp. 1–6, 2007.

[178] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[179] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, pp. 1–7, 2008.

[180] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1691 – 1708, 2012.

[181] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys Tutorials*, vol. 14, no. 2, pp. 355–379, 2012.

[182] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, p. 55–91, Dec 2011.

[183] E. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 46–52, 2012.

[184] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *2013 Proceedings IEEE INFOCOM*, pp. 2778–2786, 2013.

[185] H.-N. Dai, Q. Wang, D. Li, and R. C.-W. Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 760834, 2013.

[186] V. Milanes, J. Perez, E. Onieva, and C. Gonzalez, "Controller for urban intersections based on wireless communications and fuzzy logic," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 1, pp. 243–248, 2010.

[187] K. Wan and V. Alagar, "Context-aware security solutions for cyber-physical systems," *Mobile Networks and Applications*, vol. 19, pp. 212–226, Apr 2014.

[188] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[189] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, pp. 2294–2323, thirdquarter 2018.

[190] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, pp. 347–376, Firstquarter 2017.

[191] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 1656–1672, March 2017.

[192] S. Althunibat, R. Mesleh, and T. F. Rahman, "A novel uplink multiple access technique based on index-modulation concept," *IEEE Transactions on Communications*, vol. 67, pp. 4848–4855, July 2019.

[193] 3rd Generation Partnership Project (3GPP), "Study on Downlink Multiuser Superposition Transmission," Technical Report RP-150496, Mar. 2015.

[194] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming design and power allocation for secure transmission with noma," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639–2651, 2019.

[195] Y. Zhang, H. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, pp. 930–933, May 2016.

[196] A. Arafa, W. Shin, M. Vaezi, and H. V. Poor, "Secure relaying in non-orthogonal multiple access: Trusted and untrusted scenarios," *IEEE Transactions on Information Forensics and Security*, 2019.

[197] D. Xu, P. Ren, Q. Du, L. Sun, and Y. Wang, "Combat eavesdropping by full-duplex technology and signal transformation in non-orthogonal multiple access transmission," in *2017 IEEE Int. Conf. Commun. (ICC)*, pp. 1–6, May 2017.

[198] 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. 17, pp. 6190–6204, Sep. 2018.

[199] Z. Ding, M. Xu, Y. Chen, M. g. Peng, and H. V. Poor, "Embracing non-orthogonal multiple access in future wireless networks," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, pp. 322–339, Mar 2018.

[200] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," vol. 58, no. 1, pp. 106–112, 2020.

[201] Y. Arjoune and N. Kaabouch, "A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions," *Sensors*, vol. 19, no. 1, p. 126, 2019.

[202] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surv. Tuts.*, vol. 11, pp. 116–130, First 2009.

[203] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surv. Tuts.*, vol. 15, pp. 428–445, First 2013.

[204] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 29, pp. 877–889, Apr. 2011.

[205] M. Bouabdellah, N. Kaabouch, F. E. Bouanani, and H. Ben-Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey," *J. Inf. Security Appl.*, vol. 38, pp. 40 – 49, 2018.

[206] D. Chaitanya and K. M. Chari, "Performance analysis of PUEA and SSDF attacks in cognitive radio networks," in *Proc. Comp. Commun., Networking Internet Security*, pp. 219–225, Singapore: Springer, 2017.

[207] F. Jin, V. Varadharajan, and U. Tupakula, "Improved detection of primary user emulation attacks in cognitive radio networks," in *Proc. IEEE Int. Telecommun. Net. Applications Conf. (ITNAC)*, pp. 274–279, Nov. 2015.

[208] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 30, pp. 1850–1860, Nov. 2012.

[209] L. Qian, X. Li, and S. Wei, "Cross-layer detection of stealthy jammers in multihop cognitive radio networks," in *Proc. Int. Conf. Computing, Networking Commun. (ICNC)*, pp. 1026–1030, Jan 2013.

[210] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive

radios," *IEEE Institution Engr. Technol. (IET) Commun.*, vol. 8, no. 8, pp. 1274–1284, 2014.

[211] W. Chin, C. Tseng, C. Tsai, W. Kao, and C. Kao, "Channel-based detection of primary user emulation attacks in cognitive radios," in *Proc. IEEE 75th Veh. Technol. Conf. (VTC Spring)*, pp. 1–5, May. 2012.

[212] Y. Li, X. Ma, M. Wang, H. Chen, and L. Xie, "Detecting primary user emulation attack based on multipath delay in cognitive radio network," in *Proc. Smart Innovations Commun. and Comput. Sciences* (B. K. Panigrahi, M. C. Trivedi, K. K. Mishra, S. Tiwari, and P. K. Singh, eds.), (Singapore), pp. 361–373, Springer Singapore, 2019.

[213] N. T. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using non-parametric bayesian classification," *IEEE Trans. Signal Process.*, vol. 60, pp. 1432–1445, Mar. 2012.

[214] R. Chen, J. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 25–37, Jan 2008.

[215] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proc. 13th Annual ACM Int. Conf. Mobile Comput. Networking*, MobiCom '07, (New York, NY, USA), pp. 111–122, ACM, 2007.

[216] W. R. Ghanem, M. Shokair, and M. I. Desouky, "An improved primary user emulation attack detection in cognitive radio networks based on firefly optimization algorithm," in *Proc. 33rd National Radio Science Conf. (NRSC)*, pp. 178–187, Feb. 2016.

[217] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "Aldo: An anomaly detection framework for dynamic spectrum access networks," in *Proc. IEEE Int. Conf. Comp. Commun. (INFOCOM)*, pp. 675–683, 2009.

[218] Z. Luo, C. Lou, S. Chen, S. Zheng, and S. Li, "Specific primary user sensing for wireless security in IEEE 802.22 network," in *Proc. IEEE 11th Int. Symp. Commun. & Inf. Technol. (ISCIT)*, pp. 18–22, 2011.

[219] S. Arul Selvi and M. Sundararajan, "SVM based two level authentication for primary user emulation attack detection," *Indian J. Sci. Technol.*, vol. 9.

[220] X. Zhang, Y. Ma, Y. Gao, and S. Cui, "Real-time adaptively regularized compressive sensing in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 67, pp. 1146–1157, Feb. 2018.

[221] J. W. Choi, B. Shim, Y. Ding, B. Rao, and D. I. Kim, "Compressed sensing for wireless communications: Useful tips and tricks," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 3, pp. 1527–1550, 2017.

[222] M. Nazzal, A. R. Ekti, A. Gorcin, and H. Arslan, "Exploiting sparsity recovery for compressive spectrum sensing: A machine learning approach," *IEEE Access*, vol. 7, pp. 126098–126110, 2019.

[223] F. Ye, X. Zhang, Y. Li, and H. Huang, "Primary user localization algorithm based on compressive sensing in cognitive radio networks," *Algorithms*, vol. 9, no. 2, 2016.

[224] S. Maric, A. Biswas, and S. Reisenfeld, "A complete algorithm to diagnose and alleviate the effects of physical layer attacks," in *Proc. Int. Conf. Signals Syst. (ICSigSys)*, pp. 29–34, May. 2017.

[225] M. O. Mughal, T. Nawaz, L. Marcenaro, and C. S. Regazzoni, "Cyclostationary-based jammer detection algorithm for wide-band radios using compressed sensing," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, pp. 280–284, Dec 2015.

[226] M. A. Davenport, P. T. Boufounos, M. B. Wakin, and R. G. Baraniuk, "Signal processing with compressive measurements," *IEEE J. Sel. Areas Commun.*, vol. 4, no. 2, pp. 445–460, 2010.

[227] E. Crespo Marques, N. Maciel, L. Naviner, H. Cai, and J. Yang, "A review of sparse recovery algorithms," *IEEE Access*, vol. 7, pp. 1300–1322, 2019.

[228] M. Aharon, M. Elad, and A. Bruckstein, "K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation," *IEEE Trans. Signal Process.*, vol. 54, pp. 4311–4322, Nov. 2006.

[229] C. Jiang, H. Zhang, Y. Ren, Z. Han, K. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Commun.*, vol. 24, pp. 98–105, Apr. 2017.

[230] M. H. Beale, M. T. Hagan, and H. B. Demuth, "Neural network toolbox™ user's guide," *The MathWorks*, 2010.

[231] B. L. Sturm and M. G. Christensen, "Comparison of orthogonal matching pursuit implementations," in *Proc. 20th European Signal Process. Conf. (EUSIPCO)*, pp. 220–224., Aug. 2012.

[232] K. He and J. Sun, "Convolutional Neural Networks at Constrained Time Cost," *arXiv e-prints*, Dec. 2014.

PHYSICAL LAYER SECURITY TECHNIQUES FOR FUTURE WIRELESS COMMUNICATION SYSTEMS AGAINST EAVESDROPPING

ORIGINALITY REPORT

13%	9%	4%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

2%

★ eprints.soton.ac.uk

Internet Source

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		