Wireless LAN Security Analysis and Improvement

A Thesis Presented

By

Ephreme Tefera

To

The Faculty of Informatics

Of

St. Mary's University

In Partial Fulfillment of the Requirements
for the Degree of Master of Science

In

Computer Science

February 22, 2020

ACCEPTANCE

Wireless LAN Security Analysis and Improvement

By

Ephreme Tefera

Accepted by the Faculty of Informatics, St. Mary's University, in partial fulfillment of the requirements for the degree of Master of Science in Computer Science

Thesis Examination Committee:

____

Internal Examiner

Michael Melese (PhD)

____

External Examiner

Elefeliou Getachew(PhD)

____

Dean, Faculty of Informatics

Getahun Semeon (PhD)

February 22, 2020

DECLARATION

I, the undersigned, declare that this thesis work is my original work, has not been presented for a degree in this or any other universities, and all sources of materials used for the thesis work have been duly acknowledged.

Ephreme Tefera Weldegebreal

____

Signature

Addis Ababa

Ethiopia

This thesis has been submitted for examination with my approval as advisor.

____

Asrat Mulatu (PhD)
Signature

Addis Ababa

Ethiopia

February 22, 2020

ACKNOWLEDGMENTS

Firstly, I would like to thank God for giving me this wonderful opportunity to complete the thesis work. Even though I am confronted with a lot of difficulties to complete the task, I still managed to finish the work with great success. Then it’s time to show gratitude my supervisor, Asrat Mulatu, who helped me by guiding towards the right path by scheduling a week to week time plan. He provided me with sufficient knowledge in my study and made sure that we understand the paths without any hesitation.

Finally, a great thanks to my family who supported me and encouraged me to complete the work. I am also thankful to my friends and coworkers because they stood with me all time and helped me in every step of my decision. My friends, family and my supervisor provided me with a lot of benefits by giving ideas and comments on my thesis work so that I can prove myself with good assessment in the process. They created me a passion to work hard and accept the challenges as it leads to complete the task.

Ephrem Tefera

TABLE OF CONTENTS

LIST OF ACCRONYMS

TCP:	Transaction control protocol
UDP:	User datagram protocol
CSI:	Channel state information
RSS:	Received signal strength
LAN:	Local Area Network
WAN:	Wide Area Network
WLAN:	Wireless Network
AP:	Access Point
DES:	Data Encryption Standard
AES:	Advanced Encryption Standard
SNR:	Signal to Noise Ratio
WEP:	Wired Equivalent Protocol
MIMO:	Multi Input Multi Output
SIMO:	Single Input Multiple Output
MISO:	Multi Input Single Output

LIST OF FIGURES

LIST OF TABLES

Abstract

Due to the broadcast nature of radio propagation, the wireless air interface is open and accessible to both for authorized and illegitimate users. This is different from a wired networks, where communicating devices are physically connected each other through cables and a node without direct connection is unable to access the network. The open nature of communications medium makes wireless transmissions more vulnerable than wired communications to malicious attacks, including both passive eavesdropping for data interception and active jamming for disrupting legitimate transmissions. Therefore, this work is motivated to examine the security vulnerabilities and threats imposed by the inherent open nature of wireless communications and to devise efficient counter measure mechanisms for improving the wireless network security. We first summarized the security requirements of wireless networks, including their authenticity, confidentiality, integrity, and availability. Next, a comprehensive overview of security attacks encountered in wireless networks is presented in view of the network protocol architecture, where the potential security threats are discussed at each protocol layer. We also provided a survey of the existing security protocols and algorithms that are adopted in the existing wireless network standards. Then, we discussed the state of the art in physical-layer security, which is an emerging technique of securing the open communications environment against eavesdropping attacks at the physical layer. Several physical-layer security techniques are reviewed and compared, including information-theoretic security, artificial-noise-aided security, security-oriented beamforming, and physical-layer key generation approaches. Additionally, we discussed the integration of physical-layer security into existing authentication and cryptography mechanisms for further securing wireless networks.

Our framework is based on a hybrid of layered security based on physical primitives: collaborative jamming and the upper layer security. Notably, it can avoid the use of shared secrets, while providing a more secure system which relies on physical layer's unique features that is more secure than conventional cryptosystem.

Keywords: ***Wireless Networks, Security Framework, WLAN Security Analysis, Security Improvement***

CHAPTER ONE

INTRODUCTION

1.1 Background

A wireless LAN (WLAN) is similar to a wired LAN but radio waves being the transport medium instead of wired medium. This allows the users to move around in a limited area while being connected to the network. Thus, WLANS combine data connectivity with user mobility. In other words WLANS provide all the functionality of wired LANs, but without the physical constraints of the wire itself.

Added to the convenience and cost advantages over traditional wired network some of the benefits of wireless network include scalability, mobility, simplicity, reduced cost and installation speed. Therefore, it is necessary to provide the security of WLAN equals to wired LAN networks.

Generally a WLAN consists of a central connection point called the Access Point (AP). It is analogous to a hub or a switch in traditional star topology based wired local area networks. The Access Point transmits the data between different nodes of a wireless local area network and in most cases serves as the only link between the WLAN and the wired LAN. A typical Access Point can handle a handsome amount of users within a radius of about 70 meters. The wireless nodes, also called clients of a WLAN usually consist of Desktop PCs, Laptops, smart phones or PDAs equipped with wireless interface cards.

Wireless LAN is becoming the most popular means of network communication in our day to day life, this work illustrates the key concepts of security, wireless networks, and security over wireless networks. Wireless security is demonstrated by explaining the following specifications of the common security standards like 802.11 WEP, 802.11 WPA and WPA2 (802.11i).

Wireless communications are vulnerable to various attacks due to the open nature of radio propagation.

The inherent broadcast nature of wireless communication allows transmissions to be received by any user within the range, resulting in attackers’ ability to initiate various passive attacks such as eavesdropping, traffic analysis and monitoring, and so on, or to execute active attacks like jamming, spoofing, modification, replaying and denial-of-service (DoS) attack, etc. [1]. With the rapid increase in use of WLAN technology it is important to provide a secure communication over wireless network. Access Points can be programmed to allow access to the WLAN by MAC address [2].

Cryptography is one of the scientific techniques in information security. The word cryptography is derived from the Greek word Krypto, it means hidden thing [3]. Cryptography is very similar to both the disciplines of cryptology and cryptanalysis. This cryptography includes various techniques which involve in hiding any kind of info in storage unit or transmit the data through various ways. However in this computer specific world cryptography is related with the scrambling the normal text which is available in readable form called plaintext into unreadable text called cipher text this process is known to be encryption.

Encryption is the technique in which the readable data or original data normally called as plaintext into unreadable data or converted data called as cipher text in the term of cryptography. Plain text is in the form which is understood by any person who know the language or by a computer system. After converting this original data which is in the form of plain text into cipher text, so now no one can understand the meaning of converted data even machine cannot. By using this process we can easily share the confidential information without unauthorized expose through any channel weather the channel is secured or not [3].

The following research hypothesis are formulated to address the research problem

- The current wireless communication security mechanisms available studied
- Drawbacks of existing wireless security solutions are examined
- How today wireless technology could be secured enough so that information security, reliability, integrity and availability can be achieved?
- Exert an effort to mitigate security threat of wireless network other than traditional cryptographic methods

1.2 Statement of the Problem

Today’s wireless network security depends on cryptographic algorithms which are based on mathematical complexity of encryption key, and another problem with today’s wireless security solutions is the fact that data is still available to a third party in the medium or air so that today’s wireless security systems are more prone to unauthorized use and attack hence it require an upgrade.

Currently most WIFI, uses WPA2 (PSK) which uses SSID and pre shared key to access WLAN, which shares pre shared key between the client and access point, of course encrypted in the pathway. This key can be identified from already associated device or it can be asked from people who already has the key who are not responsible and careless to give the pass code to outsiders (it is pose vulnerability for unauthorized access).

It is common to seeing people gathered outside hotels or buildings and browsing Internet using their smart phone without permission from the owner, internet resource is utilized for unintended purpose and it has implication on cost. This indicates not only resource cost but also malicious users can easily attack the organizations information resources once they get connected by compromising the wireless connection.

It is difficult to use MAC address filtering for large offices and hotels who has frequent external users and guests It becomes laborious to register all MAC addresses exhaustively and it make it very difficult to manage large number of users in such dynamic environments, therefore this work can alleviate problems stated above and beyond

1.3 Objectives

1.3.1 General Objective

The aim of this research work is to investigate and analyze the challenges of current wireless network security limitations specially problem of eavesdropping in wireless network since WIFI uses broadcasting transmission and radio signal through air as a medium of communication as a result it is highly vulnerable to attacks than its wired counterpart, therefore it needs improving this security problem by devising a solution framework which could minimize the loopholes.

1.3.2 Specific Objectives

In order to achieve the Research goal in this study the following specific objectives are set:

- Analyze the present wireless network security features.
- Identify and point out problems of current wireless network security problems.
- Study and discover improved WLAN network security framework which has an added feature to strengthen WLAN network access security using a limited resource.
- Present the solution work and its benefit using wireless network design and or simulation tools.

1.4 Significance of the study

Information security is critical for any communication systems. Compared to wired networks, wireless communication networks face more security challenges primarily due to the nature of openness [4]. Moreover, high-level security mechanisms in wired communications cannot be directly applied in wireless communication systems. Therefore, it is certainly worth investigating techniques to secure wireless communications. Traditionally, wireless security techniques are achieved by relying solely on the upper layers of the open systems interconnection (OSI) network model. However, existing higher-layer security mechanisms are designed based on the computational hardness of mathematical functions, which are not feasible for practical wireless communication systems with limited resources. Additionally, traditional cryptographic techniques are susceptible to various types of attacks and do not directly leverage the unique properties of the wireless medium to address security threats. To this end, physical layer security has drawn a lot of attention in recent years, this security achieved based on the lowest layer of the OSI model by exploiting unique nature of physical link properties to provide additional security protections.

This research examines the existing WIFI security gaps deeply because, todays WIFI is becoming vital in our daily routine almost everywhere so it is clear that security is a great concern for data integrity, confidentiality and access control. For confidential data to be transmitted wirelessly it is advisable to use more secured communication especially where the communication medium is the air or RF signal. Physical layer security is in its infant stage that if it is further studied it could have a positive impact towards improving the drawback of wireless network to several kinds of attacks.

Therefore, using physical layer security in addition to cryptographic technique by devising a framework, which has additional feature to strengthen security, is becoming vital for these days than ever because almost all of communication is geared towards wireless in one or the other way.

1.5 Scopes and Limitations

This research examines the existing WIFI security gaps deeply because, todays' WIFI is becoming inevitable in our daily routine so it is clear that security is a great concern for data integrity, confidentiality and access control. For confidential data to be transmitted wirelessly it is advisable to use more secured communication especially where the communication medium is RF signal. Physical layer security is in its infant stage that if it is further studied it would have a positive impact towards improving the drawback of wireless network to attack.

This thesis research focus on wireless network IEE802.11 Security problems mainly on WIFI network security attack venerability issues to enhance WIFI network access for unauthorized users or malicious attackers by using physical layer security mechanism. The framework can be tested and evaluated using network design and simulation tools and recommendation would be in place. Since there are a number of wireless network security protocols and standards this thesis would focus only on physical layer security.

There is a limitation in conducting experimentation using sophisticated and fully equipped testing environment like the experiment needs USRP devices (Universal Software Defined radio Peripheral) to do experimental research in real world as the nature of the study is heavily practical , but this thesis rely on experimenting the study using simulation tools of virtual reality due to luck of those USRP devices hence forced to rely on powerful wireless network simulation tools existed MATLAB and Simulink.

1.6 Organization of the rest of the thesis

The thesis work is organized into six chapters: Chapter one focuses on the background of the study, problem statement, objectives, significant of the study and scope and limitation. In Chapter two, a range of literatures review is captured there to gather relevant information concerning wireless security issues and it is analyzed, summarized and gap analysis is also presented. In chapter three, detail of methodology followed to achieve results is outlined, it includes the study design and tools used. Chapter four cover the proposed Physical layer security framework for Wireless protocols, which is security solution for the problem identified. Chapter five evaluates the proposed conceptual framework along with the performance of the experimentation results and discuss the solution. Chapter six focus on main findings, conclusion and recommendations of the study.

CHAPTER TWO

LITRATURE REVIEW/ RELATED WORKS

2.1 Wireless Network Overview

Telecommunication has become an integral part of our daily lives and has been contributing widely to the advancement in various fields. One of the emerging mode is Wireless broadband technology which transmits multiplexed information on a wide band of frequencies. The deployment of Wireless broadband services is done by weighing the geographical population density against the bandwidth limitation. Wireless technologies are designed to reduce the time and different types of obstacles created by cables and more convenient than wired networking. In 1997,'Wireless fidelity-popularly known as Wi-Fi technology was developed by IEEE 802.11 standards which provided users the liberty to connect to the *Internet* from any place. But this service was pretty expensive till 2002 ,however the new 802.11g standards in 2003 has led to creation of WIFI enabled devices to the masses as a result today a Wi-Fi router has become a household commodity in most modern homes in India [5].

Since its inception, the Wi-Fi technology has come a long way in providing quicker wireless access to Internet applications a data across a radio network thereby making the access process faster than conventional modem. Radio bands such as 2.4GHz and 5GHz depend on wireless hardware such as Ethernet protocol and CSMA for the Wi-Fi Technology to work .Like every communication network, this method also involves transmitter (Wireless Router/Hotspot) and receiver which can be any WIFI enabled device like laptop, mobile, tablet etc. [5].

Many organizations and users have found that wireless communications and devices are convenient, flexible, and easy to use. Users of wireless local area network (WLAN) devices have flexibility to move their laptop computers from one place to another within their offices while maintaining connectivity with the network. Wireless personal networks allow users to share data and applications with network systems and other users with compatible devices, without being tied to printer cables and other peripheral device connections. Users of handheld devices such as personal digital assistants (PDAs) and cell phones can synchronize data between PDAs and personal computers and can use network services such as wireless email, web browsing [5].

2.2 WIFI Benefits

WLANs offer four primary benefits [6]:

- USER MOBILITY-Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.
- RAPID INSTALLATION-The time required for installation is reduced because network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or making modifications to the infrastructure cable plant. For example, WLANs are often cited as making LAN installations possible in buildings that are subject to historic preservation rules.
- FLEXIBILITY-Enterprises can also enjoy the flexibility of installing and taking down WLANs in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, trade show, or standards meeting.
- SCALABILITY-WLAN network topologies can easily be configured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area. Because of these fundamental benefits, the WLAN market has been increasing steadily over the past several years, and WLANs are still gaining in popularity.

2.3 Wireless network Technologies

The Wi-Fi network technology is based on IEEE 802.11 protocol. Following are the various Wi-Fi Standards [5].

- 802.11a technology has a range of 5.725 GHz to 5.850GHz with a data rate of 54Mbps.
- 802.11b with a data rate of 11Mbps at 2.4GHz.
- 802.11e addresses QOS's issues and is excellent for streaming quality of video, audio and voice channels.
- 802.11f addresses multivendor interoperability.
- 802.11g deals with higher data rate extension to 54Mbps in the 2.4GHz.

- 802.11h deals with dynamic frequency selection and transmit power control for operation of 5GHz products.
- 802.11i addresses enhanced security issues.
- 802.11j addresses channelization in Japan’s 4.9GHz band.
- 802.11k enables medium and network resources more efficiently.

2.4 Wireless Network Security attacks

WLAN-specific attacks can typically be divided into two types: passive and active. These attack classes, which are significant for monitoring purposes, are described below [6], [7].

2.4.1 Passive attack

An attack in which an unauthorized party only monitors WLAN communications; the attacker does not generate, alter, or disrupt WLAN communications. There are two types of passive attacks:

2.4.1.1 Eavesdropping

The attacker monitors WLAN data transmissions for message content.

2.4.1.2 **Traffic analysis** (a.k.a traffic flow analysis)

The attacker gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

2.4.2 Active attack

An attack in which an unauthorized party generates, alters, or disrupts WLAN communications. Active attacks may take the form of one of the following types:

2.4.2.1 Masquerading

The attacker impersonates an authorized user to gain access to certain unauthorized privileges.

2.4.2.2 Replay

The attacker monitors transmissions (passive attack) and retransmits messages posing as the legitimate user.

2.4.2.3 Message modification

The attacker alters a legitimate message by deleting, adding to, changing, or reordering the message.

2.4.2.4 Denial of service (DoS)

A DoS can occur inadvertently, such as other electronic devices causing interference, or it can occur intentionally, such as an attacker sending large numbers of messages at a high rate to flood the WLAN.

2.4.2.5 Misappropriation.

The attacker steals or makes other unauthorized use of WLAN services. We classify all WLAN attacks that target to breach one or more of the six standard security requirements on the two levels the frame level and the RF level. There are many attacks on the frame level. Table 2.1 summarizes the important wireless attacks at the frame level.

Table 2.1: Frame level Wireless attacks [16].

Attack	**Description**	**Security Element**
Man in the middle attack (MITM).	If data are unprotected, hackers can intercept data.	Confidentiality Integrity
Dictionary attack	Programs that try large passwords to get the correct one.	Authentication Access control

There are many attacks on the radio frequency (RF) level. Table 2.2 summarizes the important wireless attacks at the RF level.

Table 2.2: The RF level Wireless attacks [16].

Attack	Description	Security Element
DoS (Denial of Service)	Congesting a network resource with more requests.	Availability
IP Spoofing	If the hacker has a rogue access point with enabled DHCP, it can get IP and have access	Availability

2.5 Existing Wireless Security solutions

2.5.1 Wireless security in General

For a wired network, an attacker would have to gain physical access to network or remotely compromise systems on network, for a wireless network an attacker simply needs to be within range of wireless transmissions or nearer to the access point even outside the campus.

There are weakest Security Mechanisms, among the most commonly used security mechanisms to protect WLAN being no obstruction at all for an even unexperienced attacker are SSID hiding and MAC ADRESS FILTERING: Many APs offer user an option to hide the SSID. If it is enabled, the AP in its beacon frames does not show the SSID - an empty string is shown instead. Although it looks like a good idea (if no one sees the WLAN it cannot be attacked), it is not helpful at all. MAC ADRESS FILTERING: Like SSID hiding is also commonly used "security" mechanism. Although it is better to use even weak protection than none at all, MAC address filtering can be easily broken by using MAC address spoofing techniques [8].

2.5.2 Major Wireless Security requirements

Security aims at defending information from various malicious attacks, such as eavesdropping [9], wireless signature generation and identification, wireless key generation and distribution, wireless jamming and eavesdropping, beamforming and artificial noise, relays and cooperative nodes for secure wireless communications, and spoofing [11]. Generally, the requirements of security can be mainly divided into six categories, i.e., confidentiality, authenticity, integrity, availability, non-repudiation and privacy. Their functions are explained as follows:

- **Confidentiality**: This is also known as secrecy, which means that only authorized users can access information. This level of confidentiality should be maintained while data is transmitted from source to destination within the network.
- **Authenticity**: This means an ability of a system to validate the identities of involved users and establish trust in provided information.
- **Integrity**: This means that only authorized users can modify data in authorized ways. A system should ensure completeness as well as accuracy in all its components and prevent from unauthorized modification. 2.2. Traditional Wireless Security Techniques.
- **Availability**: This means that authorized users can access data and resources of a system in a timely manner, which ensures the reliability of all components in a system. Failing to meet this feature can cause a denial of service.
- **Non-repudiation**: This means an ability of a system to prove a certain message sent by a sender or received by a receiver, an action cannot be falsely denied by either the sender or receiver.
- **Privacy**: This is usually addressed separately from confidentiality, which means an ability of a system to protect the identities of users and enable feasible control of one's personal information by users.

2.5.3 Wireless Access Security

In this work we would focus in the different security dangers to wireless systems and conventions at present accessible like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is more hearty security convention as compared with WPA on the grounds that it utilizes the Advanced Encryption Standard (AES) encryption [8].

We use Matlab which is a wonderful tool for RF (Radio Frequency) systems design because Transient simulation is relatively easy to set up and understand, but is too slow to encompass the simulation of the full RF front end. Traditional circuit design tools do not offer the simulation.

2.5.4 WEP Security protocol

WEP Encryption: For each packet, a 24-bit initialization vector (IV) is chosen. The IV concatenated with the root key yields the per packet key. The CRC-32 is calculated over the data to be encrypted. Per packet key is then used to encrypt the data followed by the ICV using RC4 stream cipher. The (unencrypted) IV is transmitted in the header of the packet [8].

WEP Decryption: The initialization vector (IV) is unencrypted in the header. The IV is appended to the root key. The combination of IV and the root key is used as an input for the pseudo-random number generator to generate a bit sequence. This sequence is XORed with the encrypted data plus ICV to decrypt the data. The ICV calculation then is run. If the value matches the value of ICV in the incoming frame, the data is considered to be valid [8].

2.5.5 WPA and WPA2 Security

2.5.5.1 WPA (WIFI Protected Access)

The basic principle of WPA could be simplified as follows: transfer the data decrypted by Temporary Key Integrity Protocol before somebody can decrypt the key. While WEP was using single pre-shared key for all encryption, WPA changes the unicast encryption key for every frame and each change is synchronized between the wireless client and the wireless AP. For the global encryption key, WPA includes a facility for the wireless AP to advertise changes to the connected wireless clients. WPA features two different operation modes WPA-PSK (Pre-Shared Key) mode and WPA Enterprise mode.

2.5.5.2 WPA2 Security

WPA2: In September 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), which is the second generation of WPA security. WPA2 still uses PSK authentication but instead of TKIP encryption it uses enhanced data encryption: a specific mode of The Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block.WPA2, similarly to WPA, offers two modes of operation WPA2-PSK (Pre-Shared Key) mode and WPA2 Enterprise mode.

2.5.5.2.1 WPA2 Encryption

Encrypt a starting 128-bit block with data integrity key and AES.

In the next step, XOR Result1 with next 128-bit block to produce XResult1.

Encrypt XResult1 with AES and data integrity key

XOR Result2 and the next 128-bit block of data.

2.5.5.2.2 WPA2 Decryption

Decryption process can be summarized in these 4 steps:

Find the value of the starting counter from values in 802.11 header and MAC header.

The starting counter value and the encrypted portion of the 802.11 payload are used as an input for the AES counter mode decryption algorithm with the data encryption key. The result is the decrypted data and MIC. To produce the decrypted data block, AES counter mode XORs the encrypted counter value with the encrypted data block.

The starting block, 802.11 MAC header, CCMP header, data length, and padding fields are used as an input for the AES CBC-MAC algorithm with the data integrity key to calculate a MIC.

To find out if the data is valid, compare the unencrypted MIC with the calculated value of MIC. If the values do not match, WPA2 discards data.

2.5.6 IEEE 802.1X

802.1x is a protocol designed to protect a network from the user link point, such as a port of a switch in a wired network, or the access point in a wireless network. We have also seen this protocol implemented in the dynamic WEP. This protocol divides the network devices into three types:

- Supplicant is the network client that wants to connect to the network.

- Authenticator is the link point where the supplicants physically connect to the network. Commonly this device is a network switch or an access point that links the client with the network. In the client authentication process, the main role of this device is requesting and relaying authentication messages between the supplicant and the authentication server.
- Authentication server is where a client is validated. It could be any authentication server, but commonly a RADIUS server is used.

In an 802.1x-enabled network, any client that wants to initiate a network session must first authenticate before it can actually be able to be connected to the network. An 802.1x switch or access point would only permit EAP (Extensible Authentication Protocol) authentication messages; blocking any other network traffic until the user or computer completes successfully the authentication process.

WPA and 802.11i standard protocol implements this 802.1x protocol to improve the access control security to the wireless network. In addition, this protocol is responsible of generating and delivering the WPA session keys to the supplicant once successfully authenticated.

2.5.7 MAC-address access list

A stronger authentication is achieved by providing the AP with the unique MAC address that the AD carries. Each AP could be configured to contain a list of Addresses' MA addresses that are allowed to access the WLAN. Access control could be based on this rather strong authentication. It also makes it less possible that the equipment is stolen and then used on the WLAN. It exists no standard tool for updating all MAC-address lists on all APs from a

Central point. In addition to the administrative drawback, a MAC-address could easily be spoofed by a potential malicious user. Another important point is that it identifies an AD, and not a user. Although MAC-list filtering provides a strong means of identifying s it has the following drawbacks: The administration for a large network becomes very demanding since no standard for central point updating of APs MAC-address listings [12]. A MAC-address could be spoofed by a malicious user as [13]. It authenticates the network interface card, not a user.

The MAC layer enables multiple network nodes to access a shared medium with the aid of intelligent channel access control mechanisms such as CSMA/CA, CDMA, OFDMA, and so on.

Typically, each network node is equipped with a NIC and has a unique MAC address, which is used for user authentication. An attacker that attempts to change its assigned MAC address with a malicious intention is termed as MAC spoofing, which is the primary technique of MAC attacks.

Table 2.3. Main types of MAC layer attacks [24]

MAC Attacks	**Characteristics and Features**
MAC Spoofing	Falsification of MAC address
Identity Theft	Stealing of a legitimate user’s MAC identity
MITM (Man In The Middle) attack	Impersonation of a pair of communicating nodes
Network Injection	Injection of forged network commands and packets

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures. The network Security is the hottest topic in the current research scenario [14].

Abu Taha Zamani and Javed Ahmad [15], presented the use of VPN in wireless network security Virtual Private Networks (VPNs) have emerged as an important solution to security threats surrounding the use of public networks for private communications. They presents an approach to secure IEEE 802.11g WLAN using Open VPN, a transport layer VPN solution and its impact on performance of IEEE 802.11g WLAN, Throughput is slightly decreased due to the overhead increased to encapsulation and cryptographic used in Open VPN.

NPS, or Network Policy server, is one of the roles available on Windows server (2008 and 2012). It is the replacement of IAS (Internet Authentication Service) available on Windows 2003 Server. Like a RADIUS server, NPS manages authentication and authorization according to the various connection modes (local, VPN ...) It allows among other [16]:

- Access to local resources via a remote connection (VPN);
- Authentication via Active Directory;
- Rights management via GPO.

Authentication is one of the primary and most commonly ways of ascertaining and ensuring security in the network. In this work [17], an attempt has been made to analyze the various authentication techniques such as Knowledge-based, Token-based and Biometric-based etc. Furthermore, we consider multi-factor authentications by choosing a combination of above techniques and try to compare them.

Four things to consider while developing security in a wireless network namely Access, Authentication, Confidentiality and Integrity are very important. And there are different types of authentication Password and Pin based, Token based and Biometric based. To make network more secure, a combination of above techniques need to be used. This is referred to as multi-factor authentication. For network security, each authenticator result must be satisfied. As a Boolean AND operation is performed for each factors authentication results, so all must be affirmative.

Signal Processing for Wireless Network Security [10], with billions of people worldwide accustomed to daily, hourly or even constant use of wireless devices for a myriad of activities in their lives, wireless network security is among few areas of paramount importance in modern civilization. The Symposium on Signal Processing for Wireless Network Security is aimed to attract researchers from all backgrounds to come together to share their latest ideas and findings on this theme, and to promote rapid development of truly useful technologies for wireless network security.

Jae-Jung Kim et al in [11], Method of MFA (Multi Factor Authentication) for risk assessment, User authentication refers to user identification based on something a user knows, something a user has, something a user is or something the user does; it can also take place based on a combination of two or more of such factors. With the increasingly diverse risks in online environments, user authentication methods are also becoming more diversified. As hacking technologies have become more diversified and advanced, security and authentication have become unable to rely on ID and password-based authentication alone. Single-factor authentication using an ID and password has been found to be vulnerable to malware attacks, replay attacks, offline brute force attacks, key logger Trojans, and Dictionary attacks and shoulder surfing. In recent times, there has been an increase in multi-factor authentication methods based on human characteristics, such as fingerprint recognition.

2.5.8 The SSID (Service Set Identification)

Serves to identify a particular wireless network. A client that wants to join a wireless network must set the same SSID as the one in that particular Access Point. Without it, the wireless client could not be able to select and join a wireless network. Some vendors are taking this as a security measure, hiding the SSID from the beacon. Hiding the SSID cannot be considered as a security measure because it could not make the wireless network invisible and can be easily defeated using wireless network analyzers. Most wireless network analyzers are capable of obtaining the hidden SSID by passively sniffing it from any probe signal containing the SSID.

2.5.9 Cryptography

Cryptographic systems are classified into three autonomous dimensions [3]:

- **The category of processes used for converting original plaintext to cipher text**. Nearly all the security algorithm which is used for encryption process is based on couple of principals: substitution in which every element of plain text are converted into another element by using some formulae, and transposition which rearranged the elements. The basic and important requirement is that no data must be loss and after converting whenever we are trying to get back the original data through decryption it must be done properly. It means all the operation of algorithm must be reversible in every situation. Many available systems use many steps of substitutions and transpositions.
- **The number of keys used**. if in the operating sender and receiver are depend on the same secret key then that system is called as symmetric or conventional encryption as it used the single key operation. On the other side if both the user sender and recipient use different keys then the system is said to be asymmetric key or generally known as public key encryption as multiple keys are used.

- **The method by which the original plain text is handled**. A stream cipher method process the input data constantly element by element up to the end of the entire stream. In another way called as block cipher the input of single block element is process at a time and output is produced, the output is also in the form of block itself.

There are of course a wide range of cryptographic algorithms in use. The following are amongst the most well-known [18].

DES: This is the 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' system. Further Details on the DES Algorithm. 2) RSA: RSA is a public-key system designed by Rivest, Shamir, and Adleman. Further Details on the RSA Algorithm.

HASH: A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'.

MD5: MD5 is a 128 bit message digest function. It was developed by Ron Rivest. Further Details on the MD5 Algorithm.

AES: This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST.

SHA-1: SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits (20 bytes).Because of the large digest size, it is less likely that two different messages could have the same SHA-1 message digest. For this reason SHA-1 is recommended in preference to MD5.

HMAC: HMAC is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

There are also five public key cryptosystems i.e. RSA, Diffie Hellman (DH), Elliptical Curve Cryptography (ECC), Elgamal Cryptographic System (ECS) and NTRU are discussed [37].

2.5.10 Physical Layer security

Physical security PHY is studied [19] and different physical security features examined for its efficiency and effectiveness. Physical Layer Security is an increasingly important research area in wireless communications. PLS is a collection of different security techniques that seek to exploit the random nature of wireless channels to either obscure the information being exchanged over the channel and/or provide a mechanism to generate private keys that can then be used to facilitate encrypted communications.

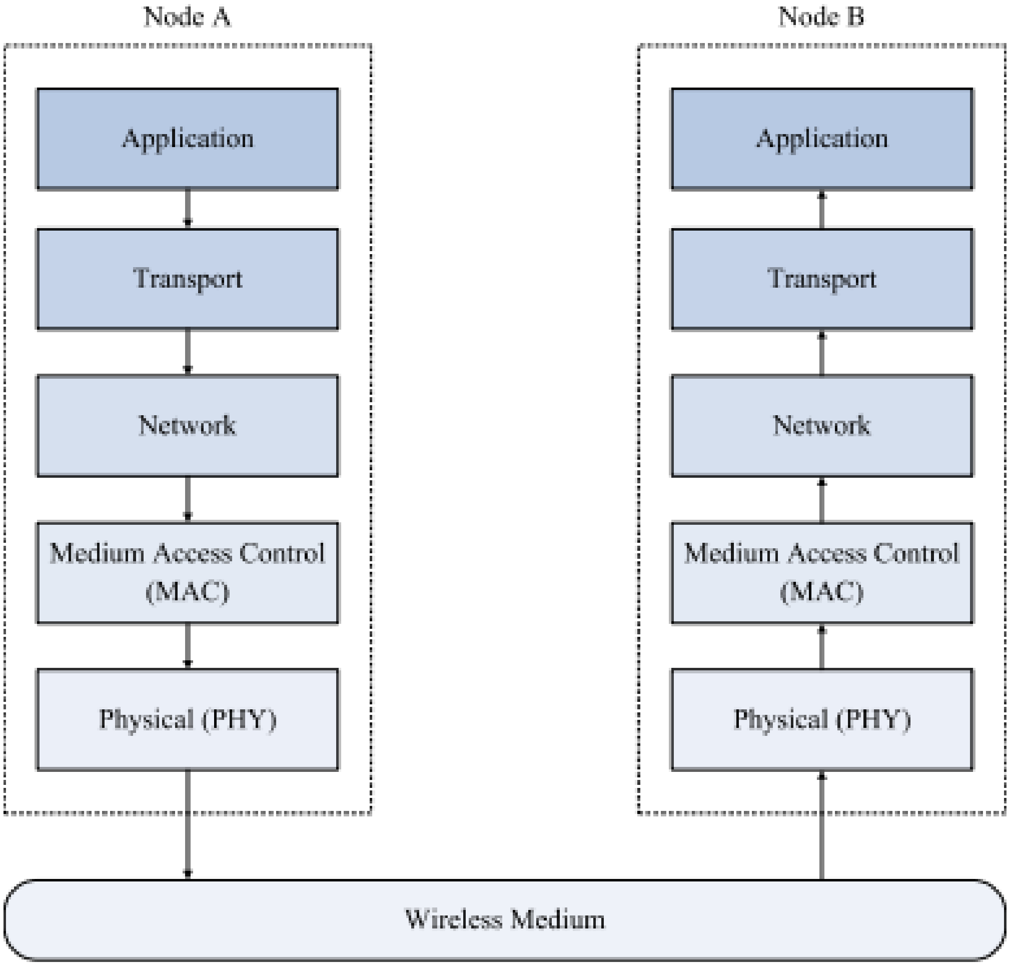


Fig 2.1: OSI Layer presentation of both wired and Wireless communication [24]

We use MATLAB and SIMULIINK which is a wonderful simulation tool for RF (Radio Frequency) systems design because Transient simulation is relatively easy to set up and understand, but is too slow to encompass the simulation of the full RF front end. Traditional circuit design tools do not offer the simulation.

2.5.11 Key Generation from Physical layer channel

Key generation from the randomness of wireless communication channels is a promising technique to share cryptographic keys securely between legitimate users. It is relatively easy to implement using off-the-shelf wireless NICs and can achieve information-theoretic security. Similar to an analog-to-digital converter (ADC), quantization in key generation is also a method to map the analog channel measurements into binary values. The quantization level QL in key generation has the same meaning as in ADC, which is the number of key bits quantized from each measurement [20].

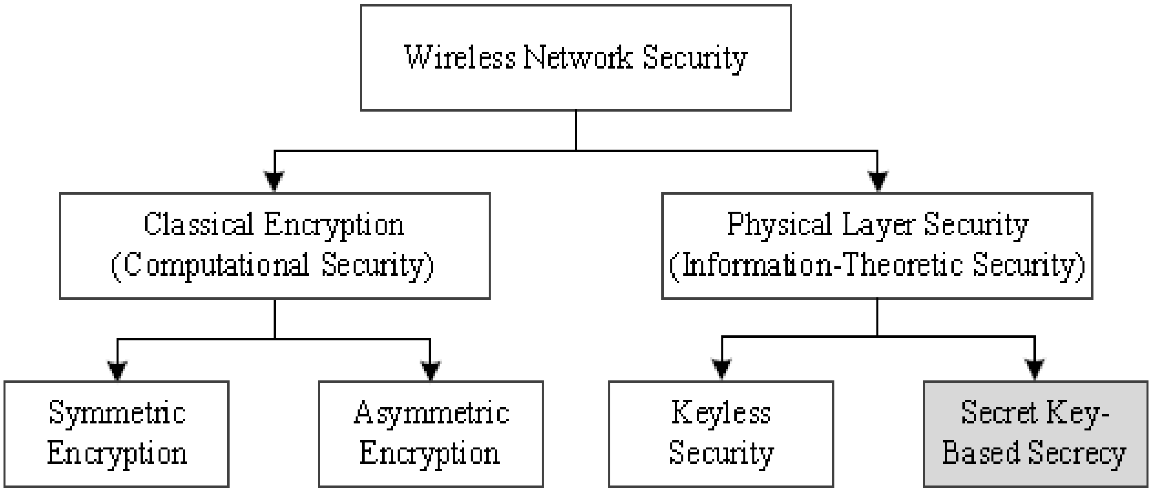

Wireless Network Security
Classical Encryption (Computational Security)
Physical Layer Security (Information-Theoretic Security)
Symmetric Encryption
Asymmetric Encryption
Keyless Security
Secret Key-Based Secrecy

Figure 2.2: Research streams in wireless network security [21].

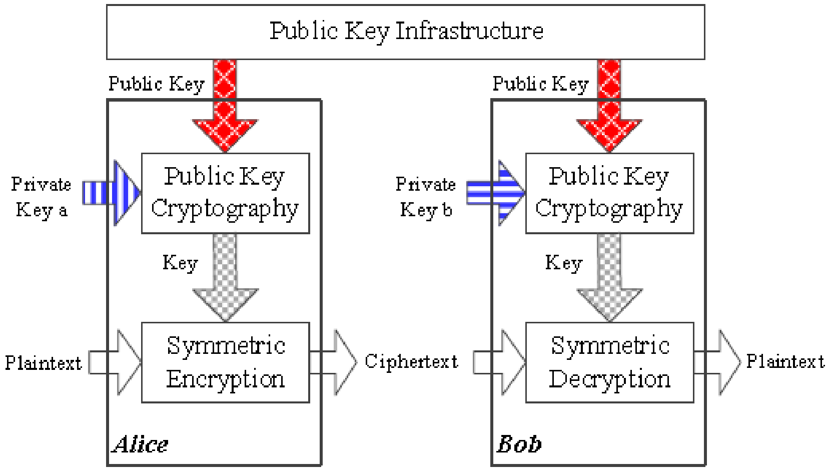


Figure 2.3: Information exchange between public key cryptography is omitted for brevity [21].

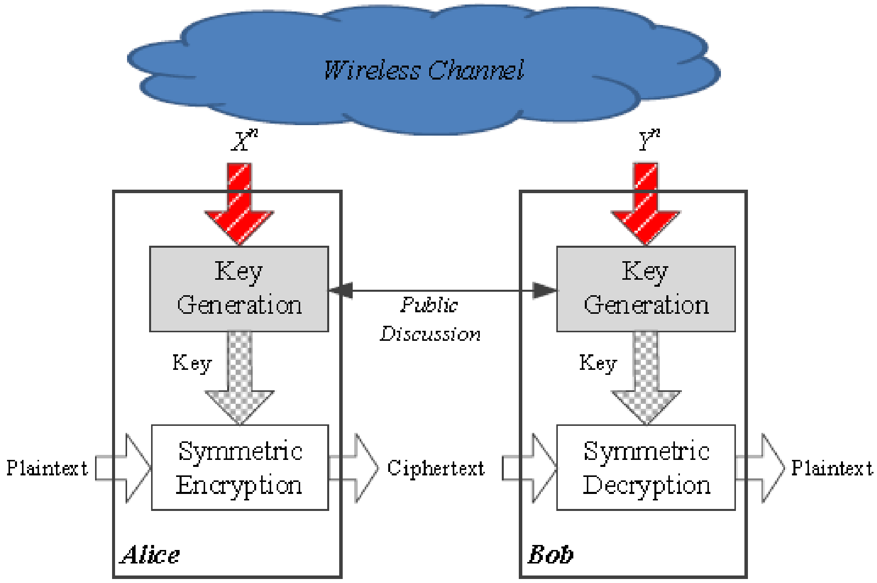


Figure 2.4: Illustration of wireless network security systems [21].

2.5.12 Security Vulnerabilities in Wireless Channels

In this section, we present the different security vulnerabilities in wireless networking systems [12]. The OSI model consists of the physical layer, the MAC layer, the network layer, the transport layer, and the application layer. The below Figure shows the generic wireless OSI layered protocol architecture consisting of the different layers through which the data packets are transmitted from node A to node B through the wireless medium.

Table 2.4. Main types of physical layer attacks [24].

PHY Attacks	**Characteristics and Features**
Eavesdropping	Interception of confidential information
Jamming	Interception of legitimate transmission

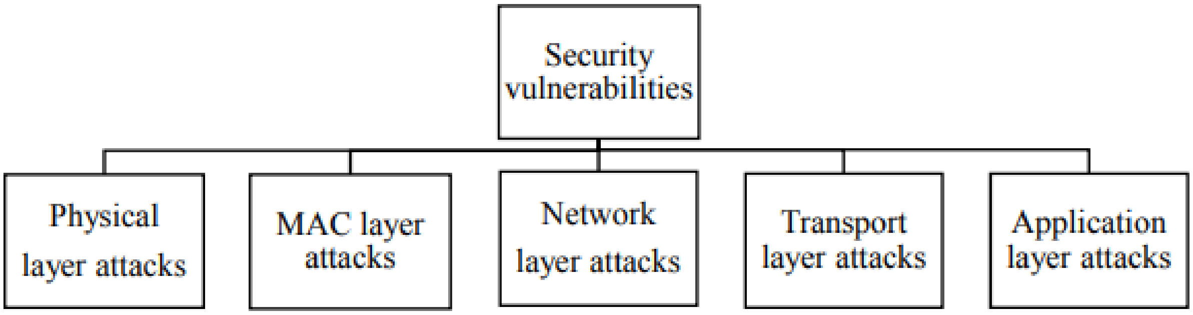


Figure 2.5: Security vulnerabilities in all layers**.**

Physical Layer Attacks: The physical layer is the bottommost layer in the OSI reference architecture through which the characteristics of the data transmission are defined. This layer is extremely defenseless to eavesdropping and other attacks. In wireless physical-layer attacks unlike [18], the eavesdropping attack is nothing but the unauthorized usage of the wireless channel without providing any license. To provide security to the confidential information, this channel must be secured from third parties like an eavesdropper.

Common attacks or vulnerabilities on physical layer are: Eavesdropping and Jamming

MAC Layer Attacks: The MAC layer allows multiple network nodes to access a shared medium using, e.g., CSMA/CA, OFDMA, CDMA, and so on. Each node has its own network interface controller, MAC address, which is used for authentication purpose.

Common attacks in MAC layer are: The attempt to change its assigned MAC address with a malicious intention known as MAC spoofing.

Network Layer Attacks: In the network layer, Internet Protocol (IP) was designed to deliver packets from the source to the destination node using their IP addresses.

Common attacks in Network layer are: IP spoofing, hijacking, and Smurf attack.

Transport Layer Attacks: In the transport layer, we have two kinds of protocols, one is TCP and the other is UDP. TCP is a connection-oriented transport protocol which is used for sending e-mails and for transferring the file from one network node to another. UDP is a connectionless transport protocol.

Common attacks on Transport layer are: Both TCP and UDP suffer from security vulnerabilities such as UDP and TCP flooding attacks and TCP sequence number prediction attacks.

Application Layer Attacks: The application layer has HTTP, FTP, SMTP etc.

Common attacks on Application layer are: HTTP attacks, FTP attacks, and SMTP attacks. HTTP attack is designed for exchanging hypertext across the World Wide Web (WWW), which as numerous security threats.

2.6 REVIEW OF RELATED WORKS

2.6.1 Related works

Sheldon, et al. [22] described how the wireless LAN encryption standards such as WEP, WPA/WPA2 are vulnerable to attack. They presented some of the attacks on encryption standards such as Chop-chop attack, Brute force, Beck-Tews, Halvorsen-Haugen and the hole 196 attacks.

V. Bhujade, et al. [3] Describe Encryption is the technique in which the readable data or original data normally called as plaintext into unreadable data or converted data called as cipher text in the term of cryptography. This system uses Encryption and Encryption algorithm therefore complexity depend on this algorithm (Complex mathematics) which uses a secret code value called Key, and

If we use the larger value of key the complexity increase. All encryption are categorized in to one of the two Substitution and Transposition and it is reversible no data is lost when decrypted. MATLAB and SIMULINK [23], well known for scripting, automation, and signal processing are tools for RF system design and analysis. These tools provide accurate estimates of RF effects and impairments within adaptive architectures as well as automated creation of behavioral models for simulation. This workflow allows you to develop and validate designs more rapidly and debug problems before building hardware prototypes.

The workflow consists of four major stages (Figure 6):

1) Static RF budget analysis.

2) Design of RF architecture.

3) System integration.

4) Validation with measured data.

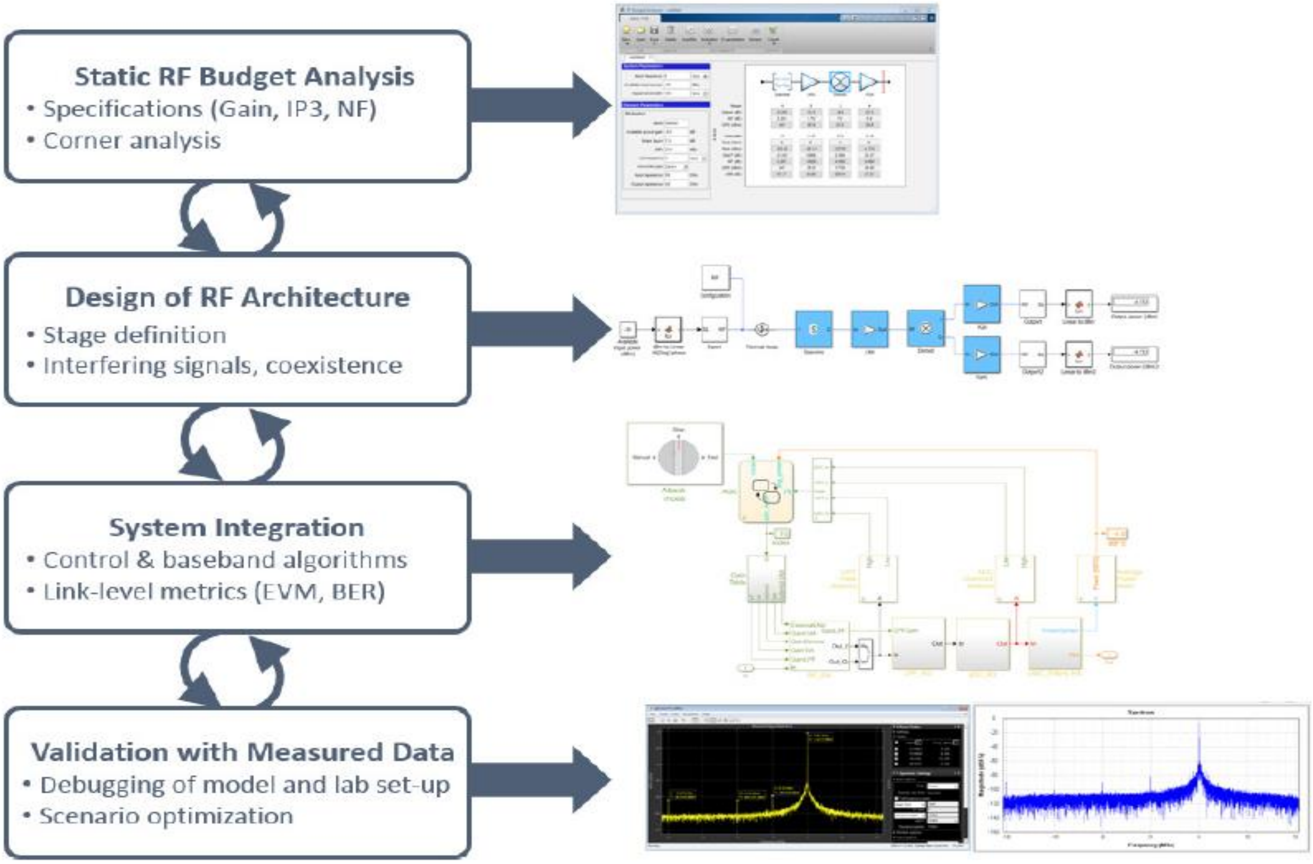

Static RF Budget Analysis
• Specifications (Gain, IP3, NF)
• Corner analysis
Design of RF Architecture
• Stage definition
• Interfering signals, coexistence
System Integration
• Control & baseband algorithms
• Link-level metrics (EVM, BER)
Validation with Measured Data
• Debugging of model and lab set-up
• Scenario optimization

Figure 2.6: Design workflow implemented in MATLAB and SIMULINK [23].

MATLAB and Simulink provide an easy-to-use, flexible, and end-to-end workflow that helps you keep up with advances, requirements, and challenges in RF system design and verification. RF Block set helps to analyze, simulate, and test an RF system before manufacturing it. With RF Toolbox and its RF Budget Analyzer app, one can calculate the RF budget to confirm the basic specifications required to design the system. Using RF Block set, one can simulate the entire RF front-end architecture including interfering scenarios and coexistence with other systems. Once you have simulated your RF architecture, you can validate it using the measurement test benches and further elaborate the model to explore scenarios, evaluate design choices, and debug prototyping problems in realistic conditions.

As in [24], present a systematic review of various security vulnerabilities and weaknesses encountered in wireless networks. Apart from their differences, wired and wireless networks also share some similarities. For example, they both adopt the OSI layered protocol architecture consisting of the physical layer, the MAC layer, the network layer, the transport layer, and the application layer as shown in Figure 1.

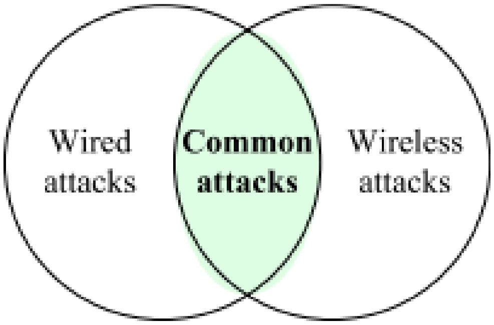
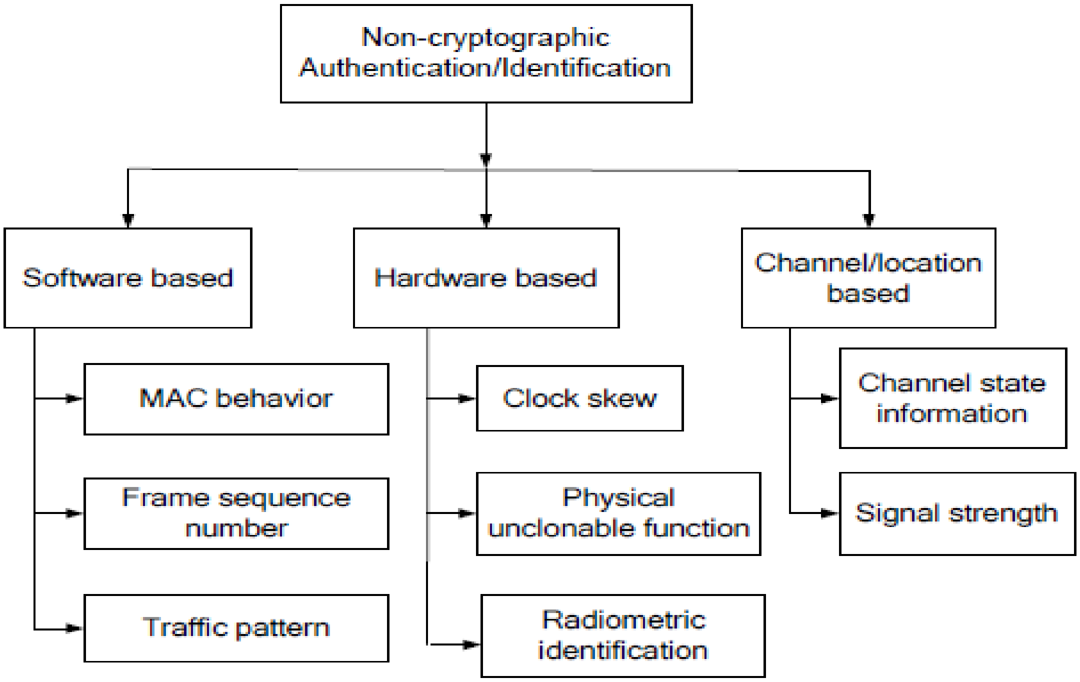


Figure 2.7: Common attacks for both Wired and Wireless communications [24].

The physical layer is the lowest layer in the OSI protocol architecture, which is used for specifying the physical characteristics of signal transmission. Again, the broadcast nature of wireless communications makes its physical layer extremely vulnerable to eavesdropping and jamming attacks, which are two main types of wireless physical-layer attacks, as depicted in Table 3. More specifically, the eavesdropping attack refers to an unauthorized user attempting to intercept the data transmission between legitimate users.

Kai Zeng, Kannan Govindan, and Prasant Mohapatra [25], Non-cryptographic wireless user authentication and device identification techniques can be broadly classified into three categories:

- Software based Fingerprinting.
- Hardware based Fingerprinting.
- Channel/Location based Fingerprinting.



Non-cryptographic Authentication/Identification
Software based
Hardware based
Channel/location based
MAC behavior
Frame sequence number
Traffic pattern
Clock skew
Physical unclonable function
Radiometric identification
Channel state information
Signal strength

Figure 2.8: Non Cryptographic authentication using physical layer characteristics.

Both channel state information (CSI) and received signal strength (RSS) have been used to identify wireless users or detect identity-based attacks. The CSI commonly indicates the channel impulse response, while RSS is usually determined by both the transmission power and the CSI. The foundation behind these schemes is that the CSI and RSS are location-specific due to path loss and channel fading. An attacker, who is at a different location from the genuine user, could incur different CSI or RSS profiles as observed by monitors/access points. Most works in this category usually assume the users are static. In a mobile scenario, these schemes could generate excessive false alarms [25].

In [9] conclusion and future works indicated that multilayer wireless security could be a solution of the future, therefore our work is based on a hybrid security framework.

2.6.2 Related work Analysis

Many of reviewed papers points that wireless network security is still a hot issue due to its broadcast nature and air or RF is the medium for communication so that anyone can get access to resources easily unlike their wired counterpart. Security solutions exist for wired network couldn't secure them well therefore Wireless security is open for research in the area and most of the works rely on theoretic aspect than dealing the issue practically.

WEP, WPA/WPA2 are vulnerable to attack, WEP is highly week so that it is no more used while EPA/WPA2 is more secure but it is still theoretically can be broken at least for brute force attack , list of attacks presented in this regard and the work concluded by suggesting layered protection approach for future.

Cryptography or scrambling of a data in storage or when it passes through a communication medium from plain text to cypher using a key and cryptography algorithm for maintaining data privacy, integrity, confidentiality and availability, use encryption algorithm with secret key to encrypt and for decryption use the same encrypting algorithm but in reverse order, for authentication you can use something you know, something you have and something you are, cryptanalysis and brute force attack is also discussed [3].

A hybrid of cryptographic techniques [23] researched to enhance the security of network as a whole but this intern improve wireless security problem since they both share common features and even similar upper layer except at the physical layer.

With MATLAB [26], [27], wireless engineering teams take algorithms all the way to full system simulation, hardware test, and implementation of WLAN, LTE, 5G, and other wireless communication systems. Using MATLAB features and products, they save time and eliminate steps by: Proving algorithm concepts in simulation and over-the-air tests with SDRs and RF instruments, Exploring and optimizing system behavior with simulations that include digital, RF, and antenna elements, Eliminating design problems before moving to hardware and software implementation, Streamlining verification by using MATLAB and Simulink models as a test harness throughout the project lifecycle Automatically converting algorithms directly into HDL or C language.

Non Cryptographic Authentication and identification [25], the idea originates from the information theoretical research, especially the research on using wireless physical channel properties for secret sharing. There has been considerable work on the wireless secret sharing problem. The idea of using wireless physical channel properties is immerging. If the adversary must have precise knowledge about the channel between legitimate users to determine the shared secrets, then any channel property that is unpredictable to the adversary can be used for secret sharing.

Method of MFA (Multi Factor Authentication) for risk assessment, User authentication refers to user identification based on something a user knows, something a user has, something a user is or something the user does; it can also take place based on a combination of two or more of such factors [28], [29].

Cryptography is solely based on computational complexity which requires high capacity hardware to compute and todays advance in computational speed doubles in 2 to 3 years that the tendency to break cryptography is becoming feasible and make it reality in the near future.

Security is a very important issue in the design and use of wireless networks. Traditional methods of providing security in such networks are impractical for some emerging types of wireless networks due to the light computational abilities of some wireless devices [such as WIFI devices, radio-frequency identification (RFID) tags, certain sensors, etc.] or to the very large scale or loose organizational structure of some networks. Physical layer security has the potential to address these concerns by taking advantage of the fundamental ability of the physics of radio propagation to provide certain types of security. This work tries to examine a recent research in this field [30].

2.6.3 Related Work Summary

This part presented related works against the required objective of the thesis work. All cover security framework on Wireless Network Security, security types for wireless network and data security solution through encryption and digital signature. From the review, since data security is about confidentiality, integrity, availability and access control of the data, those related works attempted to ensure those issues through cryptography, authentication using VPN, MFA (multifactor authentication), physical layer security for wireless network and using hybrid security. Papers revised in related works indicates that Channel State Information (CSI) and Received signal strength are the two most important pointes to deal with Physical layer security issues and previous works in this regards mainly focuses on the theoretical aspects of the solution than further realizing it as the model below.

Theory ---------→ Design --------→ Implementation-------→Evaluation

Not much work is presented in Physical Layer Security up to now and none of them bring a tangible and realistic solution yet, than laying some foundation for the problem domain.

2.6 GAP ANALYSIS

A lot of works have been done regarding securing a data in wireless networks mainly due to its broadcast nature of communication and its use of air as a medium for transmission of data it is naturally exposed to mainly man in the middle attack, there are no ultimate solutions yet regarding wireless security but many researchers stated in their future work that applying MFA (multifactor authentication), hybrid security mechanism, multilayer security and using physical layer security which requires further research towards its implementation as a solution.

Based on facts discussed above we can say that previous works on wireless security doesn’t cover the overall security issues particularly in Wireless network, There are also limitations observed so far in the related works that this work could addressed some of the limitations, in this thesis work through studying and analyzing the physical layer we propose security framework by designing wireless system.

In addition on physical layer wireless security studies most research focus on the theoretical part and no or little is done on design of PHY and I dare say none is implemented as of today. Therefore, much has to be worked beyond the theory of physical layer security.

Table 2.5: Advantages between traditional cryptographic and physical layer wireless security

	Cryptography	**Physical layer Security**
1	Designed for Wired network	Is good for wireless
2	Based on computational complexity	Solely based on the unique nature of Physical layer (CSI, RSS etc.)
3	Needs High capacity Hardware	No need of high capacity of HW
4	Exhausted/ researched	New paradigm in wireless security
5	Heavy on energy constrained devices like wireless sensors	Not costly since no need of heavy computation

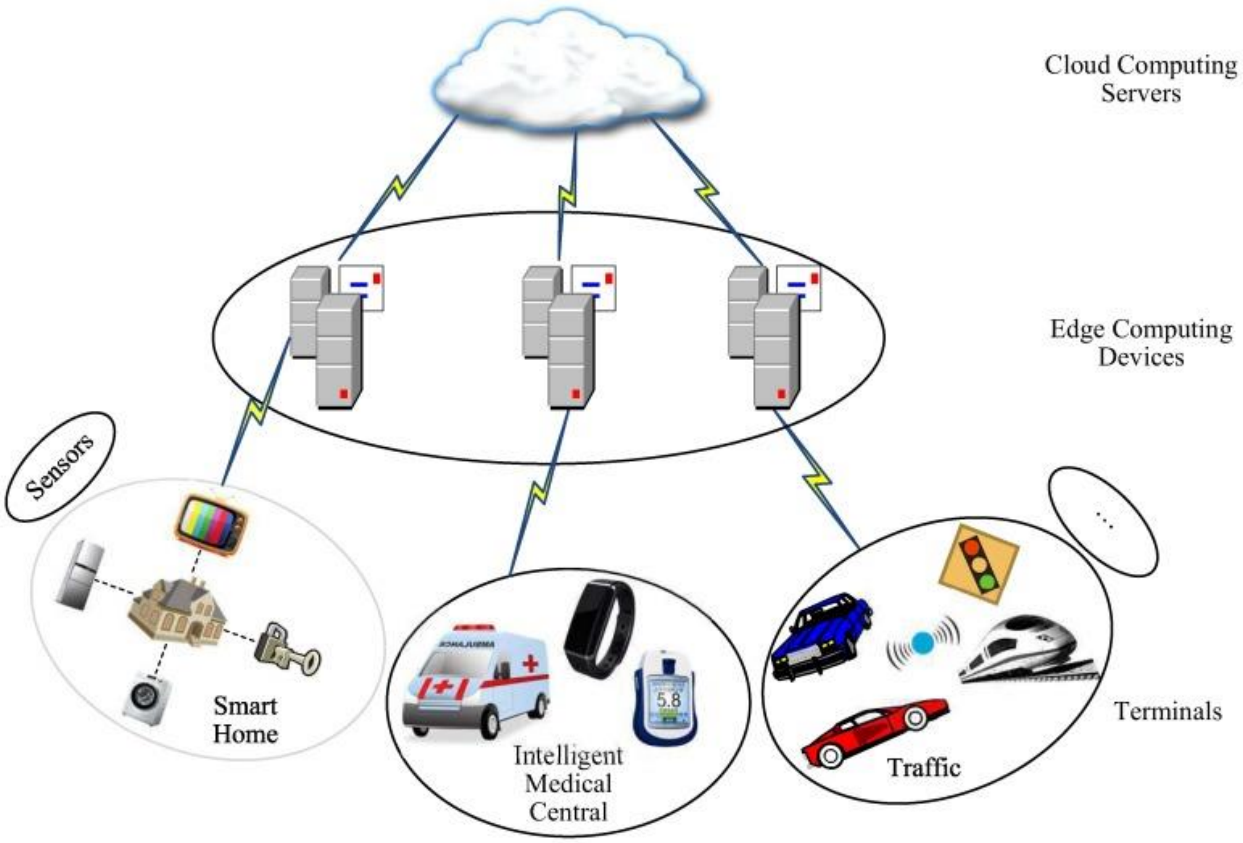


Figure 2.9: Examples of sensors and small wireless devices which suffer from high computational algorithms for security [35]

As illustrated in the figure above today’s network communication is pervasive consisting all types of devices, equipment, transportations and the likes almost all uses wireless type of network and therefore needs to be secured, focusing on wireless security is inevitable due to its open nature to several attack discussed.

CHAPTER THREE

REASEARCH METHODOLOGY

3.1 Overview

This chapter discusses the processes, techniques and tools used in carrying out the study and also provide an outline of research design especially focus on design science research.

The main aim of this chapter is to design the methodology to carry out the study, which include determining design strategy for the study including a conceptual framework, defining the deliverables, and articulating the methodology. The requirements to this study are: developing the knowledge base about the state of the problem which is wireless network security problem and the importance of its solution to define the problem and the knowledge of theory that brought to bear in a solution to design the proposed model of wireless security.

3.2 Methods

Method in this stage is a set of steps or guideline used to perform a task or in other words Methods are goal directed plans for manipulating theories so that the solution statement model or framework is realized. In order to achieve the general and specific objectives mentioned above in general and specific objectives part of this work, we use the following methods.

- Related work analysis and review: - Network security in general and Wireless network security in particular reviewed, analyzed, summarized and gap analysis is done to have broader knowledge of the problem domain, and this research problem is derived from the gaps observed in related works.

- Designing an improved wireless network security framework using physical layer security, visual paradigm could be used to design the security framework. Design Science Research is a basis for this research using design as a research method or technique [31].

- Testing security framework components and their performance, using simulation tools like MATLAB/ SIMULINK, Packet Tracer used. These tools enable us to create analysis and implement PHY (Physical layer) algorithms [16], [17].

- And finally prototype could be generated from the simulation tool itself.

Using simulation tool to measure the resulting framework since it is Experimental research. Thus the instruments used to develop the knowledge base to the study requirements are review of relevant literature including similar studies, modeling the framework and testing this solution using simulation tools.

3.3 Design Science Research

The research process model illustrated in Figure 3.1 can be interpreted as an elaboration of both the Knowledge Using Process and the Knowledge Building Process With reference to design science research effort precedes as follows:

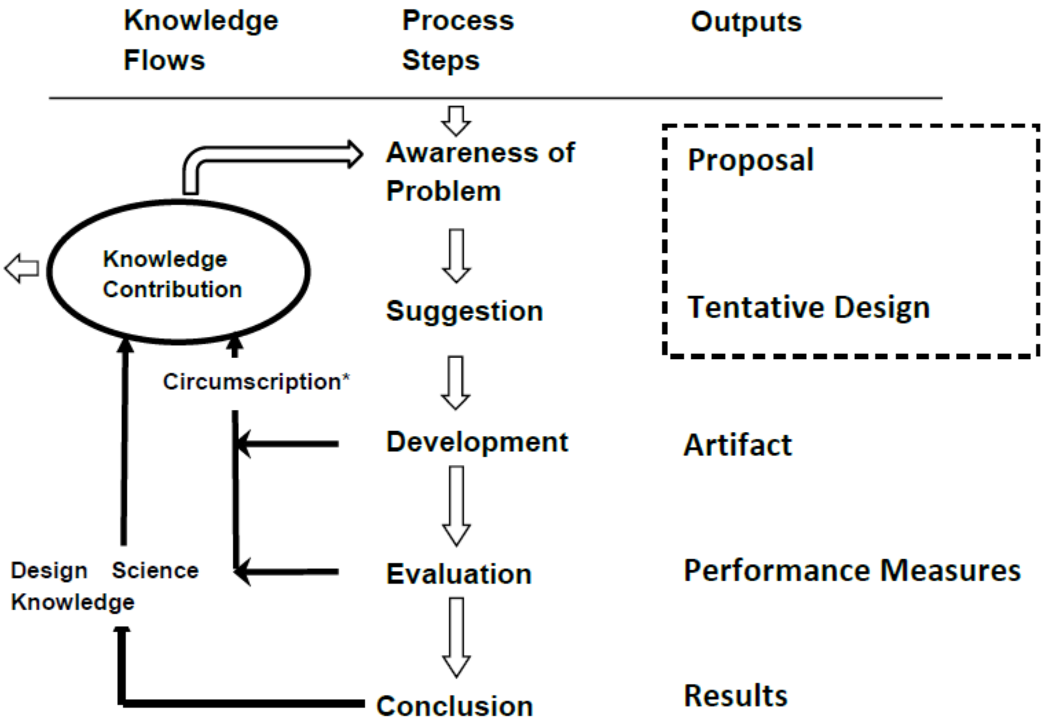


Figure 3.1: Design Science Research Process Model (DSR Cycle) [31].

Awareness of Problem: An awareness of an interesting research problem may come from multiple sources, including new developments in industry or identification of problems within a reference discipline. Reading in an allied discipline may also provide the opportunity for application of new findings to the researcher's field. The output of this phase is a Proposal, formal or informal, for a new research effort.

Suggestion: The Suggestion phase immediately follows the proposal and is intimately connected with the proposal developed based on the Awareness of a Problem.

Development: The implementation itself can be very pedestrian and need not involve novelty beyond the state-of-practice for the given artifact; the novelty is primarily in the design, not the construction of the artifact.

Evaluation: analysis either confirms or contradicts a hypothesis. Essentially, save for some consideration of future work as may be indicated by experimental results, the research effort is over.

Conclusion: This phase could be just the end of a research cycle or is the finale of a specific research effort. The finale of a research effort is typically the result of satisficing, that is, though there are still deviations in the behavior of the artifact from the (multiple) revised hypothetical predictions; the results are adjudged "good enough." Not only are the results of the effort consolidated and "written up" at this phase, but the knowledge gained in the effort is frequently categorized as either "firm"—facts that have been learned and can be repeatedly applied or behavior that can be repeatedly invoked—or as "loose ends"—anomalous behavior that defies explanation and may well serve as the subject of further research.

The output of a design science research project should be design science knowledge. To understand what form this knowledge contribution can take it is good to start with understanding the possible types of knowledge contribution of design science research [31].

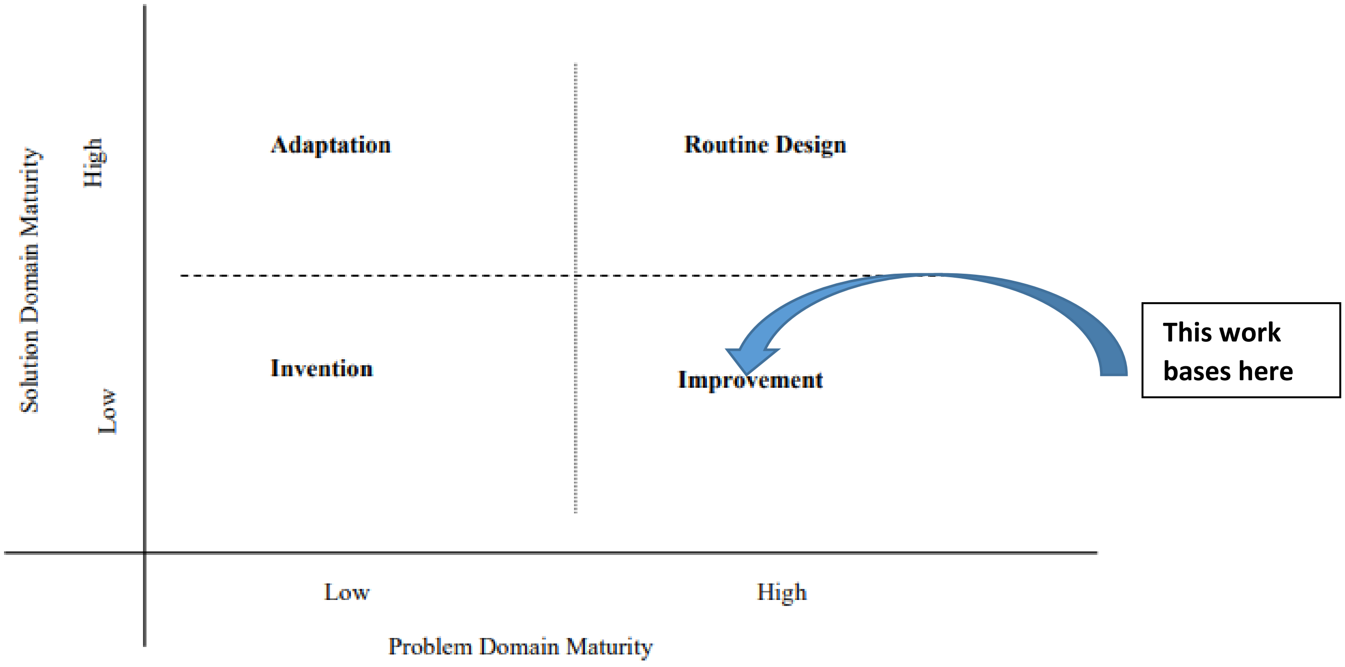


Figure 3.2: Design science knowledge contribution Framework [31].

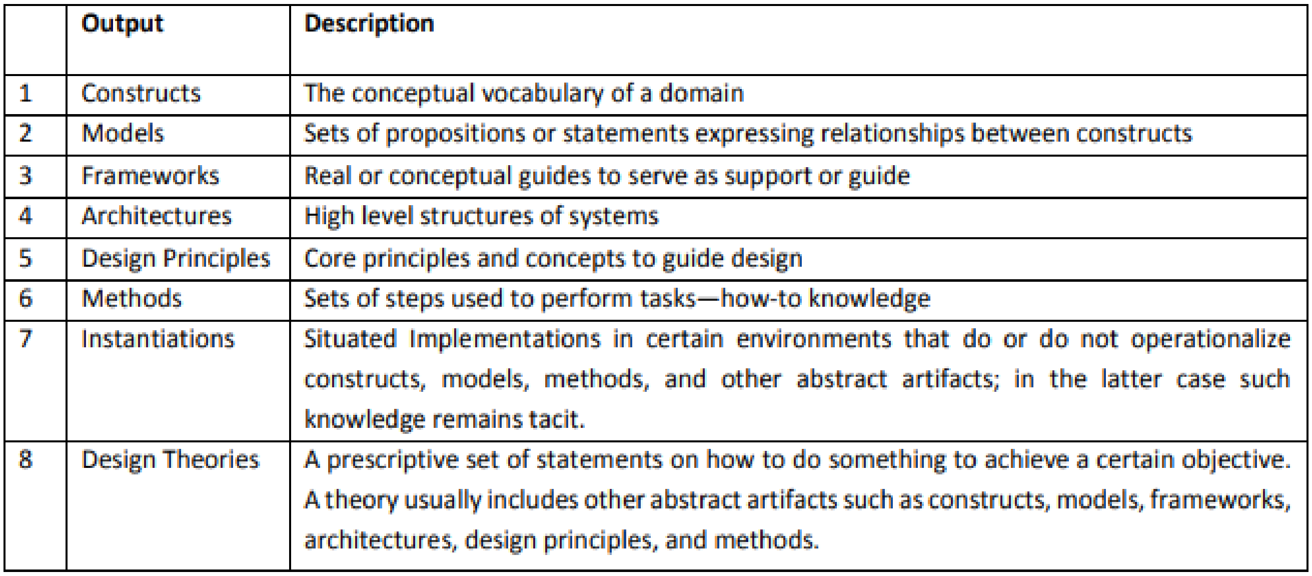
We conduct literature studies in the area of computer network security to get a broader understanding of the domain in which this thesis work base. Then further study on literatures and other related works about WLANs security, in doing so review papers written on different journals, conference proceedings and refer Institute of Electrical and Electronics Engineers (IEEE) 802.11 WLAN security standards. This intern lead us to analyze and see the gaps further and try to fill those pities and formulate improvement framework in the security of 802.11 WLAN and specifically device criteria to evaluate complementary techniques to WLAN network using network tools for experimentation.

The study is mainly focused on Physical layer security in which apply stronger framework of layered algorithms to further strengthen the security of WIFI networks communication.

The proceeding studies reviewed in the area of the various techniques that complement IEEE 802.11 standard. These could be evaluated with enhancement framework and recommendations followed based on the criteria. The recommended solution could be used to make an 802.11 WLAN more secure.

Output of design science research

Table 3.1: Output of design science research's list [31].



	Output	**Description**
1	Constructs	The conceptual vocabulary of a domain
2	Models	Sets of propositions or statements expressing relationships between constructs
3	Frameworks	Real or conceptual guides to serve as support or guide
4	Architectures	High level structures of systems
5	Design Principles	Core principles and concepts to guide design
6	Methods	Sets of steps used to perform tasks—how-to knowledge
7	Instantiations	Situated Implementations in certain environments that do or do not operationalize constructs, models, methods, and other abstract artifacts; in the latter case such knowledge remains tacit.
8	Design Theories	A prescriptive set of statements on how to do something to achieve a certain objective. A theory usually includes other abstract artifacts such as constructs, models, frameworks, architectures, design principles, and methods.

Natural science has a traditional focus on truth whereas design science research focuses more on (situated) utility.

3.4 Tools used

MATLAB and SIMULINK is used in this thesis work because since this security framework deal with Physical layer, the encoding and transmission of data over the wireless medium is the main purpose of the PHY layer thus it is suitable in that it can simulates the RF using MATLAB's Wireless tool which has many features including (beamforming, artificial noise, zero-forcing, and convex optimization) as if it is happening real, of all the simulation tools currently available in that.

Many wireless engineers rely on MATLAB® to develop algorithms, analyze data, explore new technologies, and publish thousands of research papers and contributions to the MATLAB Central community site. The reason is that MATLAB is ideal for physical layer modeling, the foundation of all wireless systems [36]

CHAPTER FOUR

IMPLEMENTATION OF THE PROPOSED WIRELESS SECURITY FRAMEWORK

4.1 Overview

A Framework is theories which are formulated to explain, predict, and understand phenomena and, in many cases, to challenge and extend existing knowledge within the limits of critical bounding assumptions. The theoretical framework is the structure that can hold or support a theory of a research study [32], it is real or conceptual guides to serve as support or guide, natural science has a traditional focus on truth whereas design science research focuses more on (situated) utility. Thus a model is presented in terms of what it does and a theory described in terms of construct relationships. However, a theory can always be extrapolated to what can be done with the implicit knowledge and a set of entities and proposed relationships can always be expressed as a theoretical statement of how or why the output occurs.

Designing the details of the upper layer security and their layered security processes are not the scope of this research because it is well studied and understood, the focus of this study is to use physical layer (unique channel property) along with the traditional upper layer security with this improving the security.

Key management, dealing with cryptographic techniques and broadcast nature of wireless networks make it difficult to get ultimate solution for its security problem so that a number of solutions proposed are being used to get stronger security, this proposed framework solution can improve.

4.2 Proposed Framework

Many researchers have been used different frameworks in the study of adopting new technological innovation. Among frameworks that have been developed based on the past studies that are well received framework in the context of innovation adoption have been used in many studies are discussed below.

The theoretical framework of the research included the different components of the framework helped to identify the propositions to be tested and also guided the analysis and geared the research to answer the research questions with regard to wireless security enhancement. These frameworks are basically a "blueprint" for building a Wireless Security standard to manage risk and reduce vulnerabilities. Information security pros can utilize these frameworks to define and prioritize the tasks required to build security into especially on wireless security [33].

Described below is the general Hybrid security framework of physical layer security and the above layers security standards combined together for a better security result.

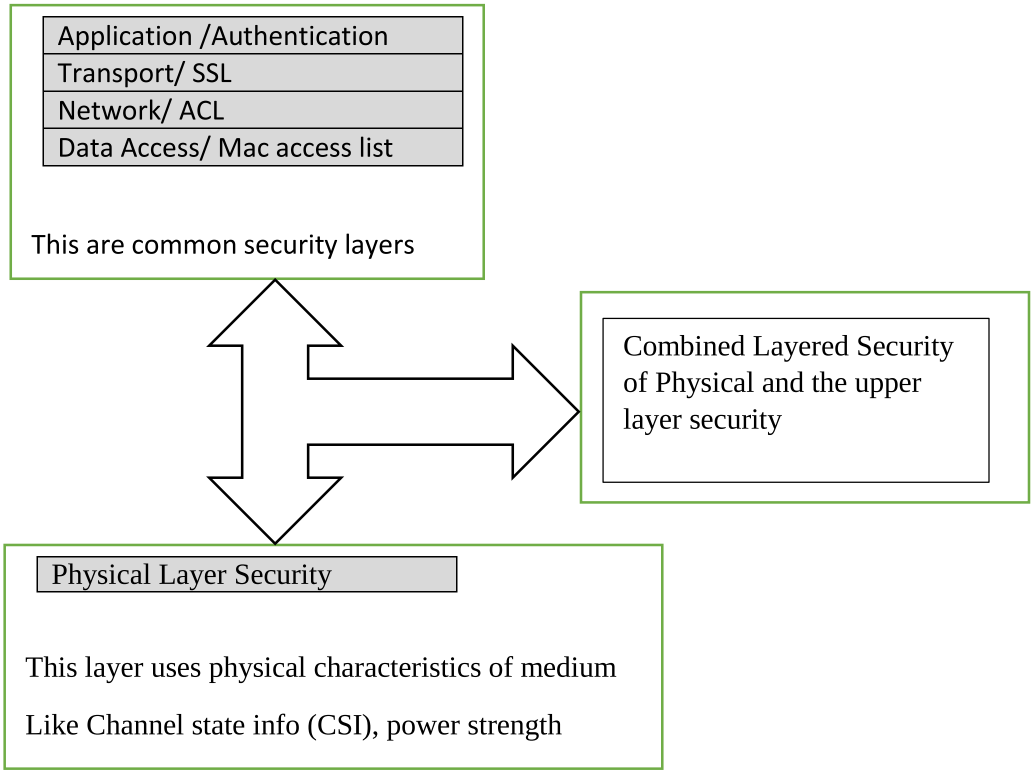

Application /Authentication
Transport/ SSL
Network/ ACL
Data Access/ Mac access list
This are common security layers
Combined Layered Security of Physical and the upper layer security
Physical Layer Security
This layer uses physical characteristics of medium
Like Channel state info (CSI), power strength

Figure 4.1: Conceptual framework for hybrid Wireless network security using Physical layer and the upper layers security together.

This general framework is based on the strength of physical layer security which is new and less researched in this area since it eliminates key sharing problem. As [34] the implications of eliminating shared-secrets for achieving secure communications and it has various benefits such as:

- the key management overhead is greatly reduced (if not eliminated) when there is no shared secret at all;
- shared secret-free physical layer security can be seen as a way of increasing the security level of wireless networks wherein, say for reasons of resource limitation, a highly secure protocol cannot be implemented at higher layers;
- it can be used as a building block in efficiently bootstrapping the security parameters and configuration data required by higher layer protocols and applications; bootstrapping is widely regarded as being a hard and important problem for deeply embedded and potentially large scale wireless networks;
- Finally, it is conceivable that in some application scenarios that it is possible to completely avoid the use of shared-secret based cryptosystems.

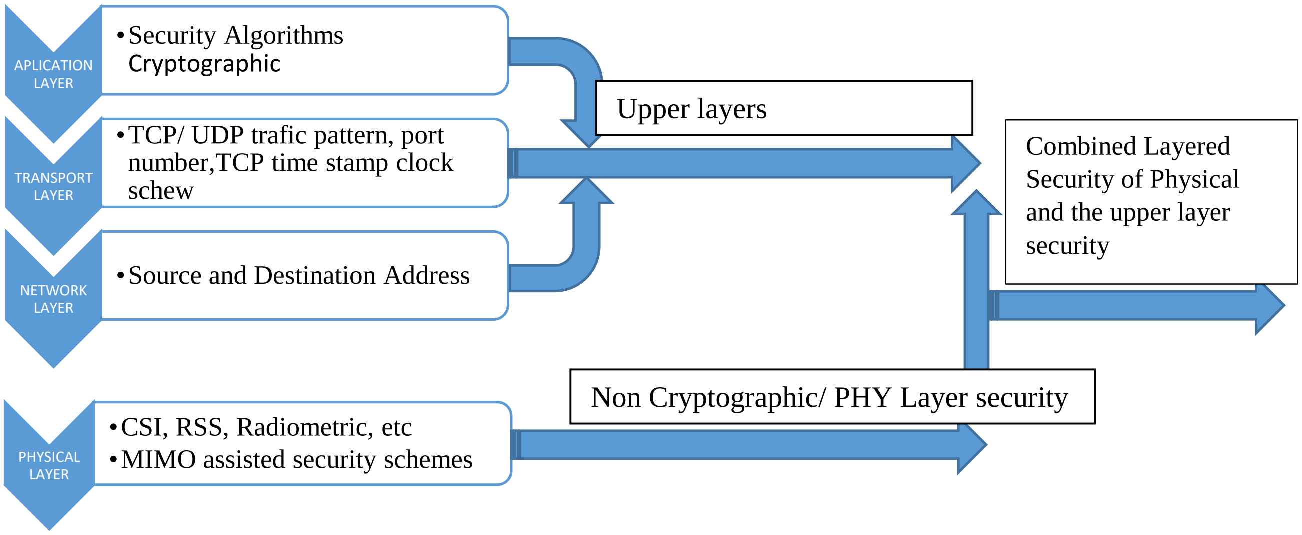

APLICATION LAYER
•Security Algorithms
Cryptographic
TRANSPORT LAYER
•TCP/ UDP trafic pattern, port number,TCP time stamp clock schew
NETWORK LAYER
•Source and Destination Address
PHYSICAL LAYER
•CSI, RSS, Radiometric, etc
•MIMO assisted security schemes
Upper layers
Non Cryptographic/ PHY Layer security
Combined Layered Security of Physical and the upper layer security

Figure 4.2: Illustration of each layers security and their Hybrid security model

Since cryptographic technic is well studied for years and exhausted we focus our study on realization of physical layer security to just combine and hybridize these two and get strong security scheme by aligning the advantages from each scenarios. To do these a scenario called Alice, Bob and Eave are used just Alice is transmitter, Bob is receiver and Eave is eavesdropper or unintended user of the link as shown in the diagram below.

4.3 Framework Narration

This framework uses one or more of the upper layer cryptographic security and hybridize it with the physical layer security using XOR logic to meet both security checks though the upper layer security is not covered in this work, that is for a receiver to communicate with sender uses one of traditional security algorithm like cryptography but this is not enough to be considered legitimate user, receiver should also agree using one of the physical layer security mechanisms or channel fingerprinting (RSS, CSI etc.).

It uses Physical layer security instead of using digital secret keys cryptography, it utilizes various non-replicable features of channel conditions and attributes of signals for security enhancement. From those physical features introduction of certain percent of nose to the channel is used and optimized to increase the capacity of legitimate transmission channels between legitimate sender and receiver to decrease the capacity of illegitimate transmission within the channels.

For ease and simplicity reason we don’t see cryptography security systems mainly because it is not the scope of this work since it is well studied in previous times, what we do is simply combine it with physical layer security for its untapped and unique features which is new in the area of wireless and is not exhaustively studied yet.

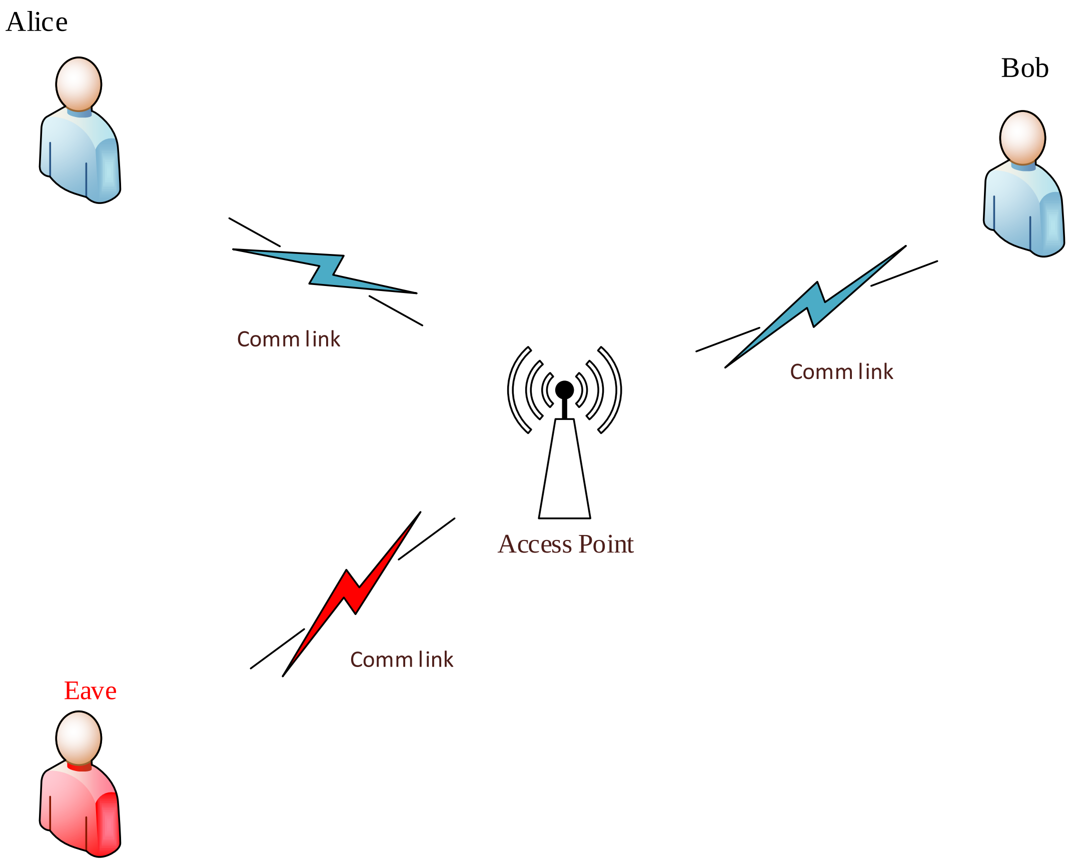


Figure 4.3: Alice Bob and Eve communication scenario.

Alice and Bob are two legitimate users of wireless link whereas Eave is eavesdropper or illegitimate user who sniffs the network for unintended purpose, the idea is that both Alice and Bob knows the channel state information of the link so that they can communicate each other but Bob in the other hand has no information about the link information so that it is difficult for Bob to get clear signal and demodulate to get the information.

Process flow diagram of recommended framework is shown below

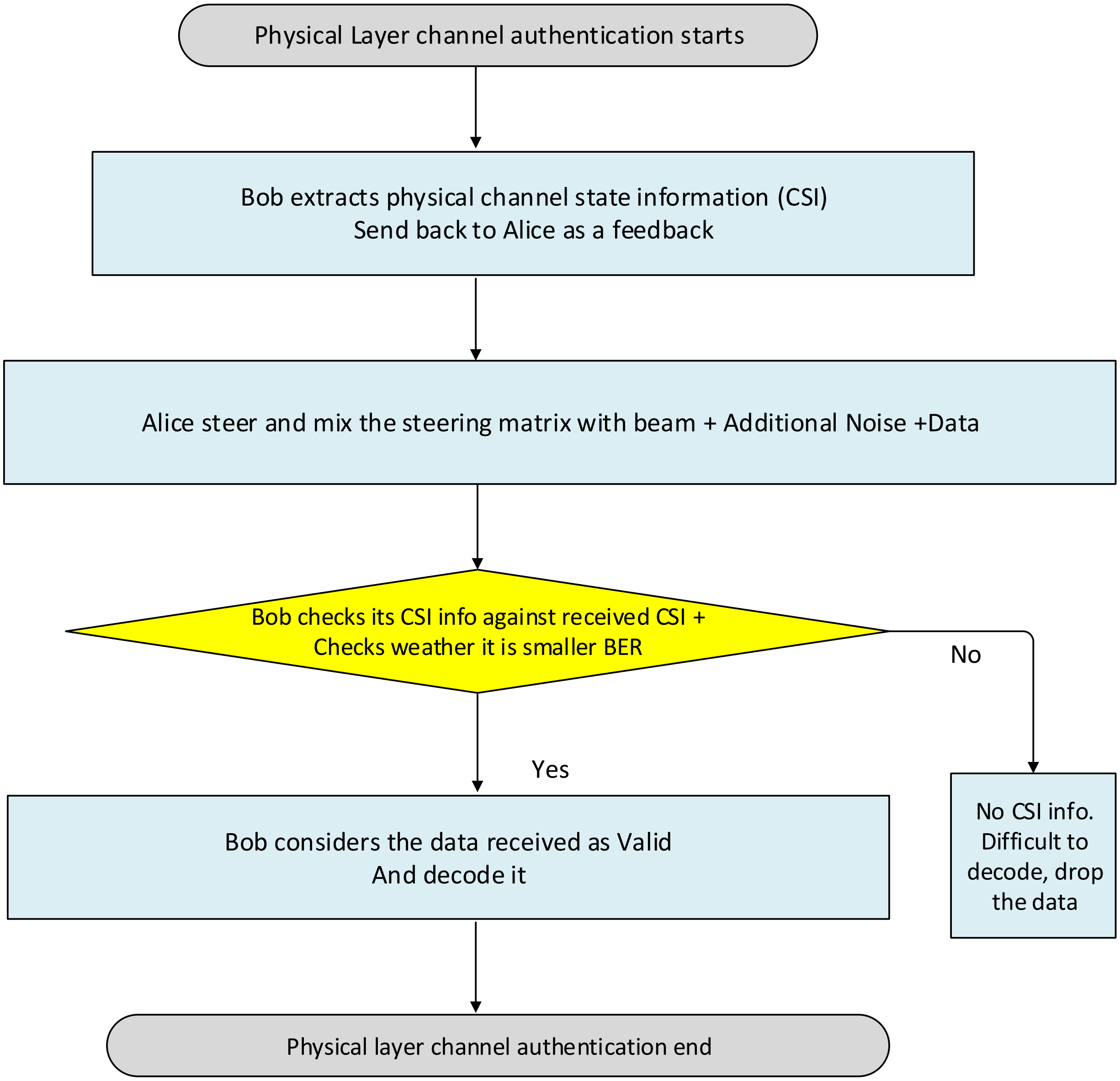

Physical Layer channel authentication starts
Bob extracts physical channel state information (CSI)
Send back to Alice as a feedback
Alice steer and mix the steering matrix with beam + Additional Noise +Data
Bob checks its CSI info against received CSI +
Checks weather it is smaller BER
No
Yes
Bob considers the data received as Valid
And decode it
No CSI info.
Difficult to
decode, drop
the data
Physical layer channel authentication end

Figure 4.4: Process flow chart of proposed physical layer security.

The above Physycal layer channel authentication is narrated as below

When Bob receives a new data frame, it can directly verify the legality of the data frame according to the established physical-layer channel model figure above and the process flowchart of physical-layer channel authentication. The detailed authentication principle of physical-layer security model is summarized below.

- Bob extracts the channel information from the received data frame sent from Alice, where, the channel information is a complex matrix of *m* rows and *n* columns, the data frame contains the cipher text and “⊕” means XOR function, and indicates the index of data frame.
- Bob preprocesses the channel information to obtain the statistical characteristics of channel information, Bob accumulates the absolute value of the real part and the imaginary part, respectively.
- Bob checks the validity of the data frame between his and Bob and the central position respectively. Then, Bob compares the sizes, Bob considers the data frame to be valid and that belongs to him according to (physical-layer channel model); otherwise, Bob drops the data since it has higher BER so that bob couldn’t decode it.
- Cryptographic authentication is not presented here because it well studied so far and it is not the main purpose of this work.

4.4 Proposed System Implmentation Using MATLAB simulation tool

- This work is experimented using MATLAB and SIMULINK which are the most useful simulation software especially for dealing with physical layer simulation, noisy cannel simulation is illustrated shown on Figure x: and it shows SNR signal to noise ratio is an important variable which can be used to use as unique property or physical layer’s figure printing and one can filter by calculating signal to noise ration using filters in MATLAB.
- In addition to normal SNR we introduce additional noise on the transmitter which eligible communicators both Alice and Bob has information about it but not unintended users in this case Eve.

4.4.1 Use of Beam formed signal regarding transmiting to the intended receiver

- This experiment shows how the security of wireless link can be improved by using beamforming the transmission when channel state information is available at the transmitter.

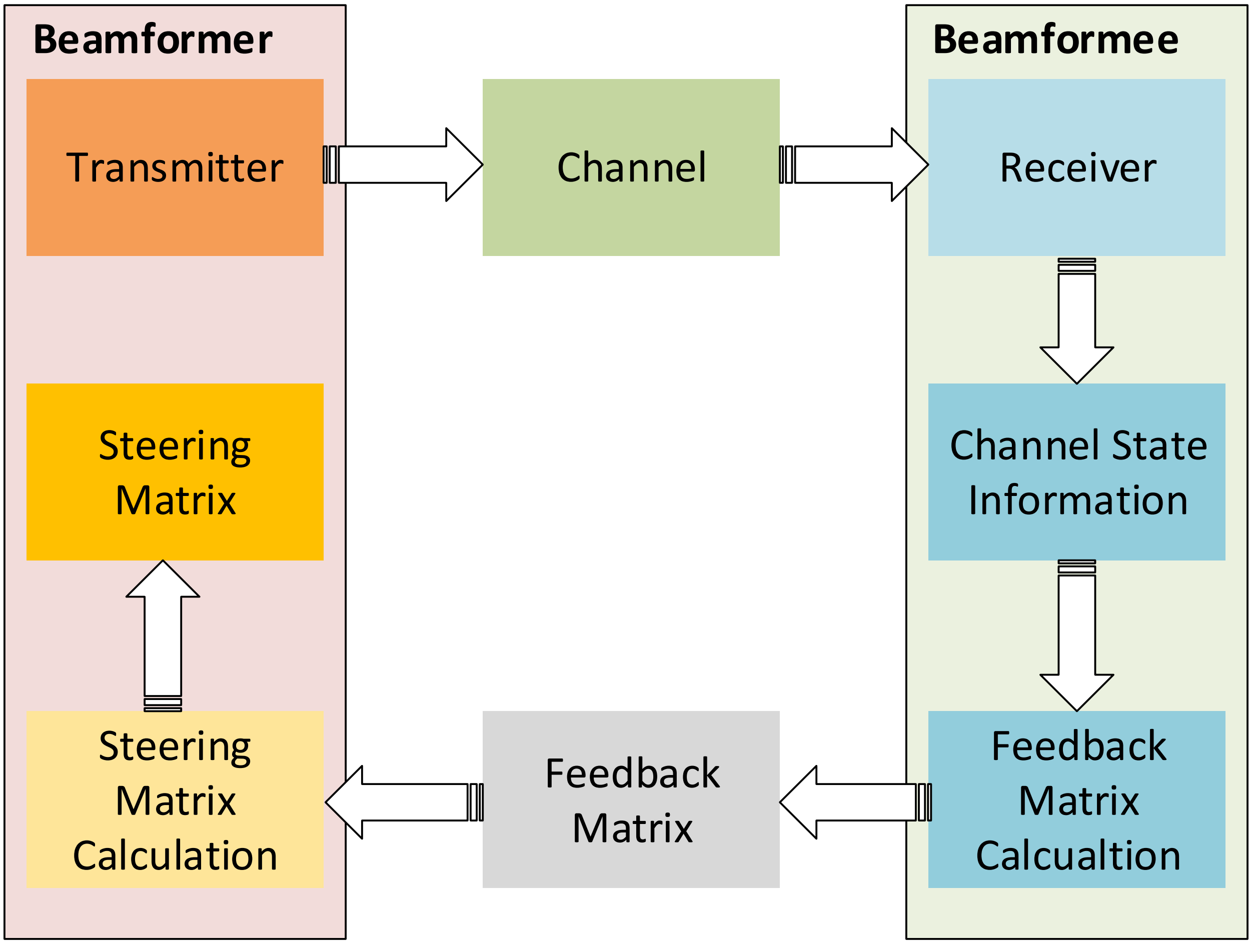

Beamformer
Beamformee
Transmitter
Channel
Receiver
Steering Matrix
Channel State Information
Steering Matrix Calculation
Feedback Matrix
Feedback Matrix Calcualtion

Figure 4.5: Process of forming the steering matrix.

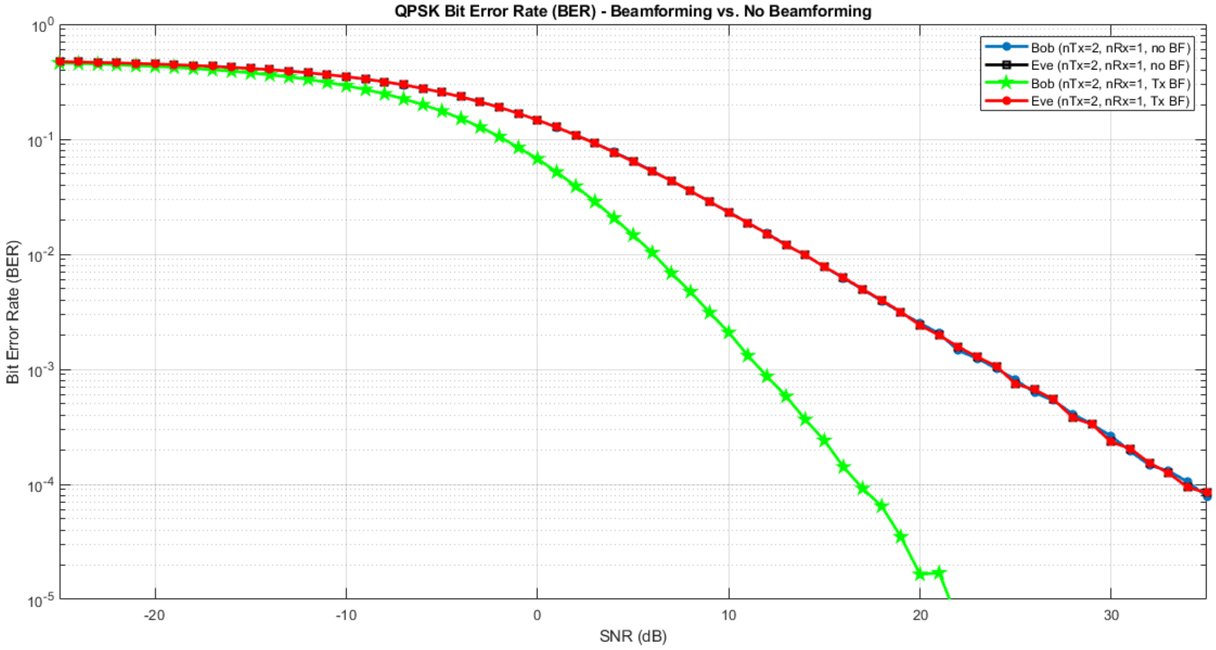


Figure 4.6: Multi input single output (MISO) Beamforming versus non Beamforming output

This MATLAB script provides a comparison between a MISO 2 x 1 antenna simulated system's performance and that of simulated Tx beamforming for a MISO 2 x 1 system containing the following actors Alice (transmitter) has 2 Tx antennas, and Bob (intended receiver) has 1 Rx antenna and Eve (unintended receiver i.e. eavesdropper) has 1 Rx antenna. The result shows on no beamforming both Bob and Eve has the same bit error rate (BER) whereas on beamforming scenario Eave has the same BER as no beam forming but Bob shows much lower bit error rate meaning Bob can easily demodulate the signal and get the information easily while Eve not as the constellation diagram in MATLAB shown below.

Bit error rate is the measure of performance of a digital communication system, which characterizes the reliability of the radio system through bits “in to out”. The concept of bit error rate (BER) is simply given by

BER = Errors/Total Number of Bits

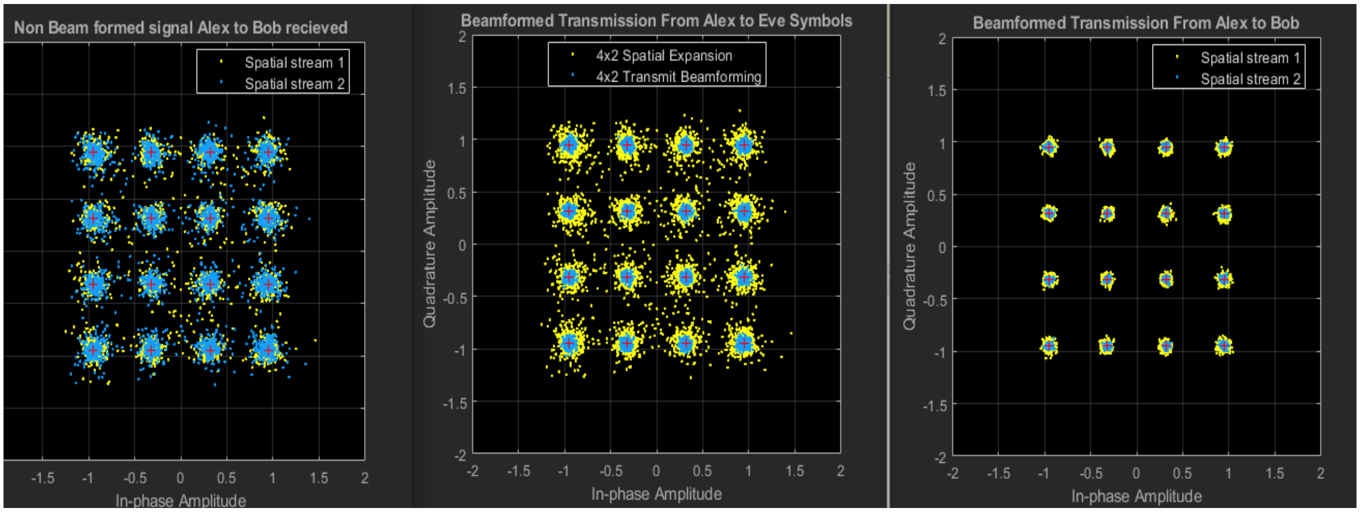


Figure 4.7: Constallation diagram of transmission with and without beam forming

The above constellation diagram shows how Transmit Beamforming shows the performance of wireless link can be improved by beamforming the transmission when channel state information is available at the transmitter and this performance variance ratio can be used as CSI difference so does decoding efficiency of beam formed signal increased.

Transmit beamforming focuses energy towards a receiver to improve the SNR of a link. In this scheme the transmitter is called a beam former and the receiver is called a beamformee. A steering matrix is used by the beam former to direct the energy to the beamformee. The steering matrix is calculated using channel state information obtained through channel measurements. These measurements are obtained by signaling the channel between beamformer and beamformee. To sound the channel the beamformer sends a Null Data Packet to the beamformee. The beamformee uses the channel information provided by signaling to calculate feedback matrix. This matrix is feedback to the beamformer in a compressed format. The beamformer can then use the feedback matrix to create a steering matrix and beamform transmissions to the beamformee.

A 4x2 MIMO configuration is used in this example with 2 space-time streams. The format specific configuration of a VHT waveform is described using a VHT format configuration object. In this example the waveform is configured with a 20 MHz bandwidth and the MIMO configuration specified above. The variance in the constellation with no beamforming is approximately the same for each spatial stream as the SNRs are approximately the same. This is because the average power in the channel is on average approximately the same per space-time stream but the variance between Bob and Eve with beamforming is different.

4.4.2 Use of Additional Noise to transmission medium

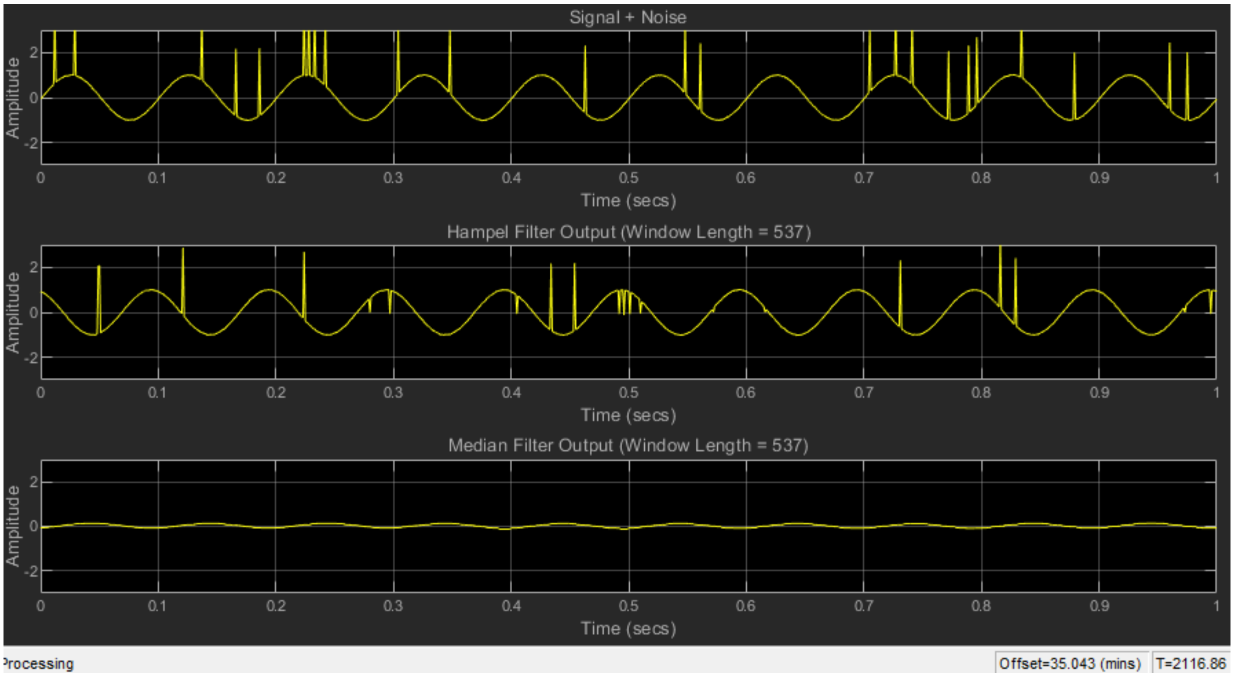


Figure 4.8: Spectroscopic reperesentation of wireless signal with and without noise in MATLAB.

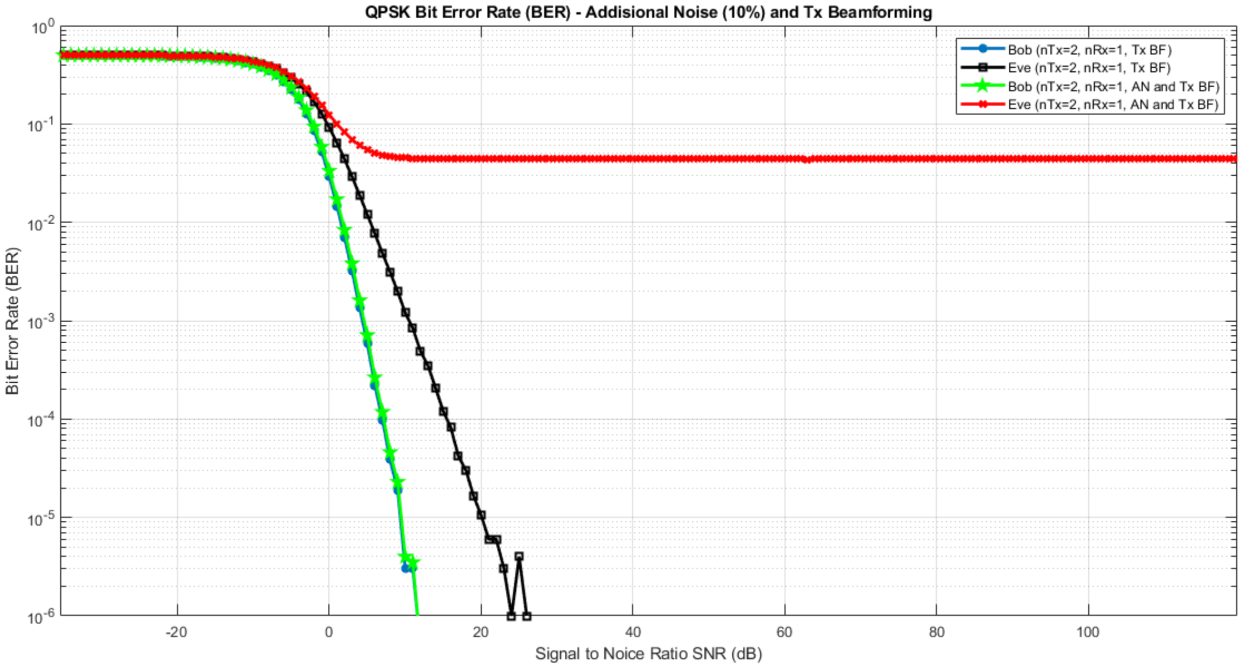


Figure 4.9: QPSK modulation which is bemformed and additional noise of 10% of total energy added

Table 4.1: Output of Bit Error rate to SNR from MATLAB experimentation at 10% of noise addition

SNR in dB	BER at Bob	BER at Eve
-30	0.01	0.30
-20	0.3	0.30
-10	0.6	0.15
0	0.05	0.10
10	10^{-6}	0.03

The result from the above MATLAB simulation which uses 10% on noise, the output shows lower BER for Bob but also Eve has significantly lower BER especially when SNR value increases. So we don’t take this as a good secrecy between Alice and Bob because Eave can still get the information due to its lower BER.

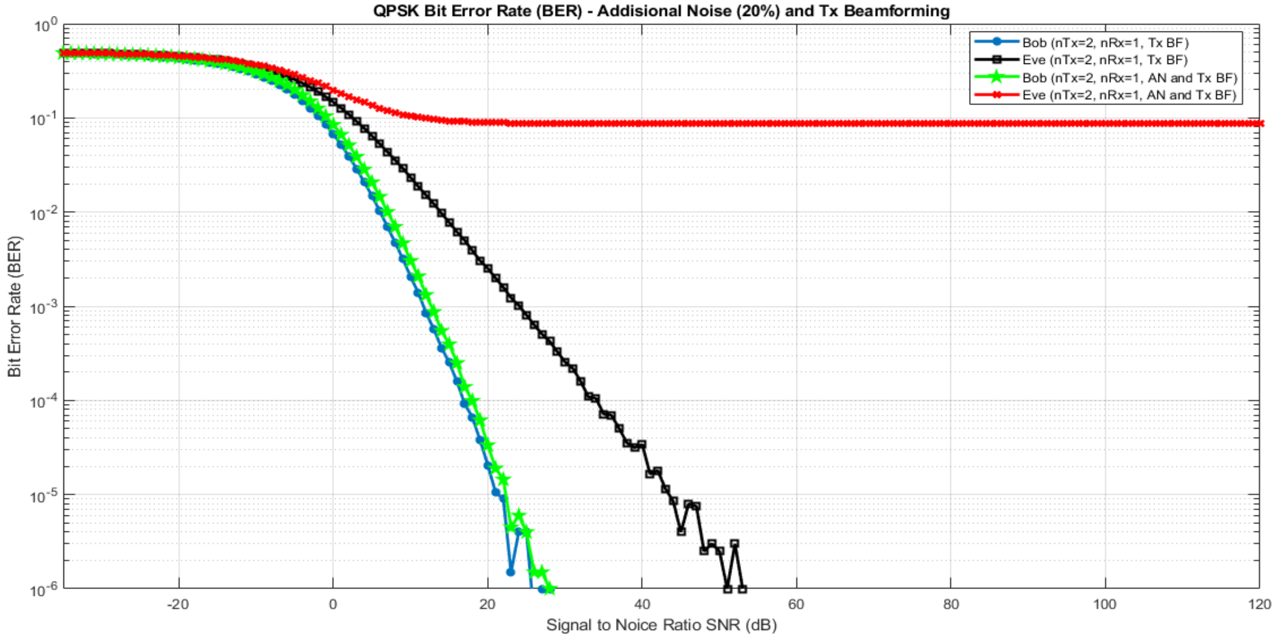


Figure 4.10: QPSK modulation which is bemformed and additional noise of 20% of total energy added

Table 4.2: Output of Bit Error rate to SNR from MATLAB experimentation at 20% of noise addition

SNR	BER at Bob	BER at Eve
-10	0.5	0.6
0	0.09	0.33
10	0.05	0.1
20	0.0005	0.1
30	10^{-6}	0.1
40	-	0.1
50	-	0.1

The result from the above MATLAB simulation which uses 20% of noise, the output shows a lower BER for Bob but also Eve has significantly lower BER even though the value a bit higher than from 10% noise experiment result. So, we don't take this as a good secrecy between Alice and Bob because Eave can still get the information due to its relatively lower BER which is 0.1 on average.

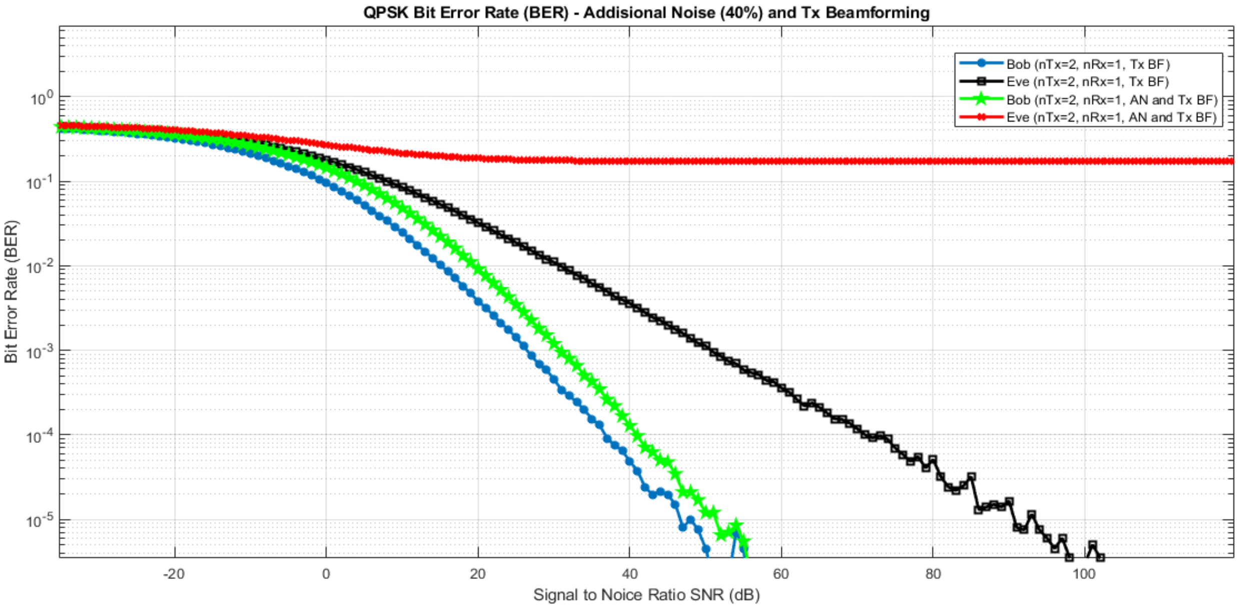


Figure 4.11: Output of Bit Error rate to SNR from MATLAB experimentation at 40% of noise addition.

Table 4.3: Output of Bit Error rate to SNR from MATLAB experimentation at 40% of noise addition.

SNR in dB	BER at Bob	BER at Eve
0	0.12	0.50
10	0.085	0.40
20	0.01	0.30
30	0.001	0.30
40	10^{-4}	0.30
50	10^{-5}	0.30
60	10^{-6}	0.30

The result from the above MATLAB simulation graph and table which uses 40% of noise, the output shows a lower BER for legitimate Bob but Eve has significantly higher BER even the value is higher than from 20%. So, we take this as a good secrecy between Alice and Bob because Eve can’t get the information due to its higher BER 0.3 or higher on average.

Meaning BER = Error Bits/Total Bits

To elaborate 0.3 means 3/10 therefore, out of 10 bits 3 are errors, therefore one cannot decode and get transmitted data if the error is this much high, in the same way Eve can’t get the transmitted data even though it can decode it.

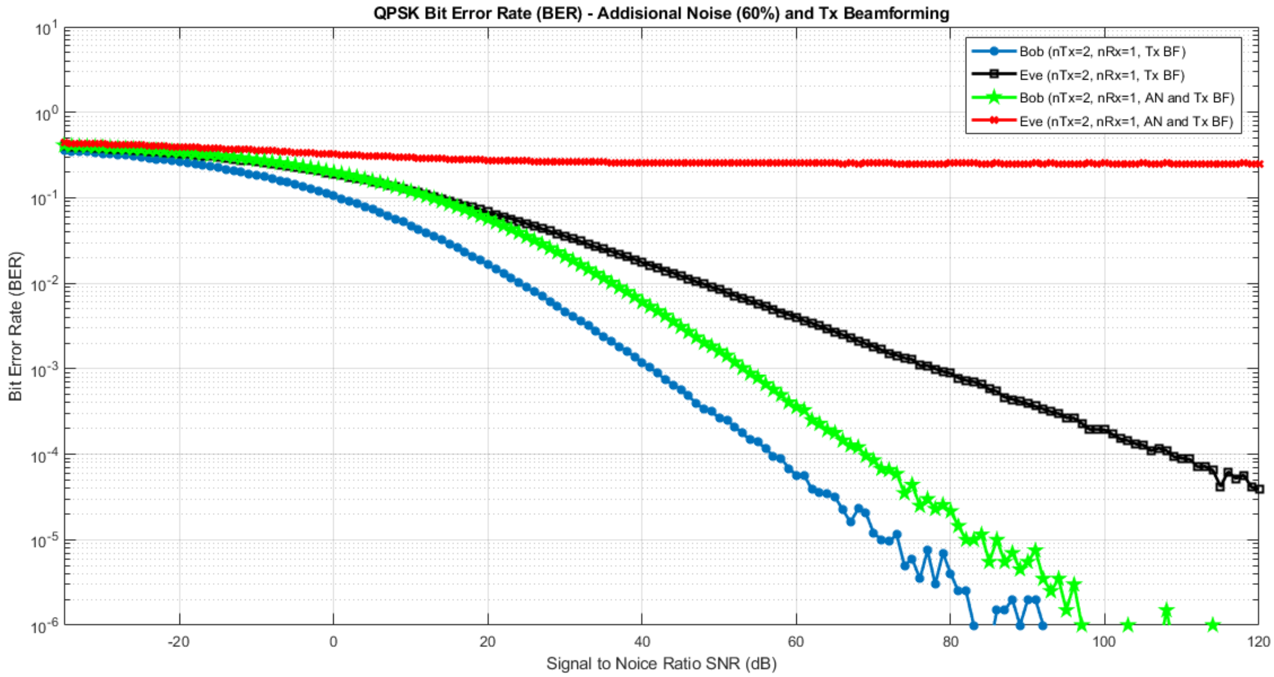


Figure 4.12: Output of Bit Error rate to SNR from MATLAB experimentation at 60% of noise addition.

Table 4.4: Output of Bit Error rate to SNR from MATLAB experimentation at 60% of noise addition.

SNR	BER at Bob	BER at Eve
-10	0.400	0.600
0	0.250	0.500
10	0.130	0.424
20	0.081	0.424
30	0.043	0.424
40	0.007	0.424

The result from the above MATLAB simulation which uses 60% of noise, the output shows a relatively high BER for Bob and Eve also has very significantly higher BER 0.45 on average even the value is a bit higher than from 40%. So, we cannot take this as a good secrecy between Alice and Bob because Bob can’t get the information due to its relatively higher BER 0.1 or higher on average. In addition, we cannot take noise level of the higher proportion to the actual data signal power so that we can’t consider this for a secrecy.

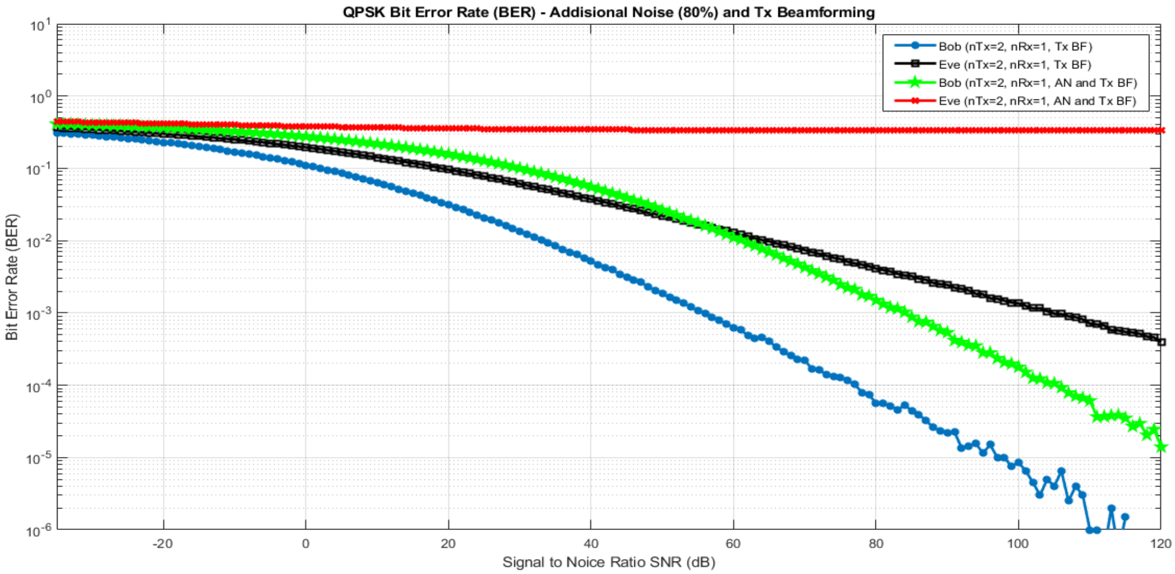


Fig 4.13: Output of Bit Error rate to SNR from MATLAB experimentation at 80% of noise addition.

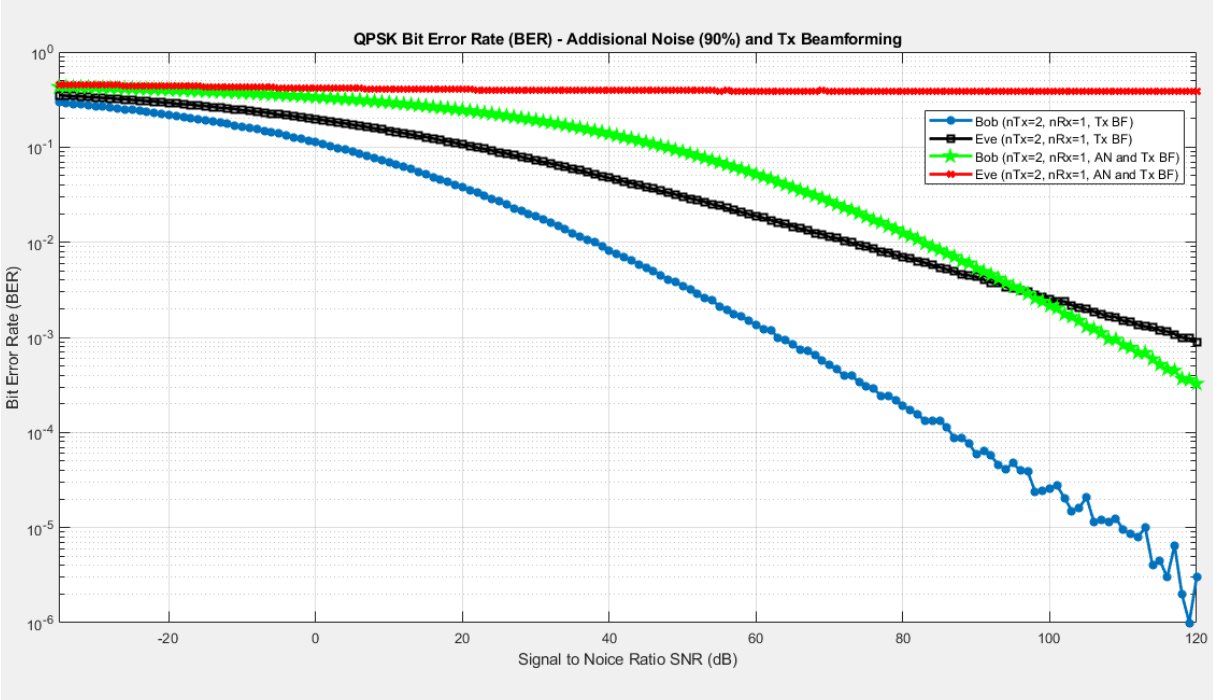


Figure 4.14: Output of Bit Error rate to SNR from MATLAB experimentation at 90% of noise addition

CHAPTER FIVE

RESULTS AND DISCUSSIONS

5.1 Evaluation

In this, work results of the proposed framework of secure communication between Alice and Bob with the third party unauthorized user eavesdropper Eve, the result in the graph and table between legitimate user and Eve is shown in the channel simulated the proposed method using MATLAB simulation results, through Bit Error Probability (BER) of both Bob and Eve with the channel mismatch which is visible enough to distinguish the difference with a higher Bit Error rate on Eve and relatively very low or little BER on Bob observed. The desired result of generating beamforming and further introducing additional noise on transmitter side which is Alice is to degrade the channel of potential eavesdroppers other than intended receiver Bob that means while degrading eavesdropper Eve's signal at the same time not impacting the quality of the channel of the intended receiver Bob.

It is important to note that even in a scenario where Eve's SNR is increased, the secrecy provided could remain the same since the increased SNR of Eve could not only provide her with a stronger information signal but with increased secrecy of signal which is introduced on transmitter observed by her as well this impacted the quality of signal received by Eve which intern degrade the Bit quality received when decoded to get the right data transmitted from Alice.

In the meantime Bit Error rate of Eve increased or remains the same at significant level even while SNR keeps increased this means it is too difficult for Eve to decode the signal she received and get the right data traversed through the channel, by doing this secrecy capacity of the channel is increased by introducing additional noise in the transmission channel.

As it is shown on simulation result the injection of additional noise which is further beam formed entails the sender Alice generating some limited additional noise and transmitting that noise in all directions other than in the direction of the intended receiver Bob.

5.2 Performance of the system

To examine the performances of the proposed framework scheme, we firstly simulated it in MATLAB under different signal-to-noise ratios (SNRs). In the simulations, we set the maximum Doppler shift of 15 Hz, the bandwidth of 1 MHz, the digital modulation method of QPSK, the number of subcarrier 128, the number of multi-paths 2, and 102 times with noise percentage level of 0, 10%, 20%, 40%, 60%, 80% and even 90% test a total of 102 times for those different scenarios.

Simulation result in the previous chapter shows that different level of additional noise introduced and 40% of noise level to total signal power is optimum and gives a better result in that achieve higher secrecy capacity at this level than other levels, our recommendation is to use 40% of noise to signal proportion at which we get best secrecy capacity of 94.0% of accuracy. In previous works we don't see its accuracy level and therefore this works result can be used as a basis for such studies. This experiment work tries to see all percentage levels 0 up to 100 but it is very insignificant when used in less than the difference of 10, that is why 10%, 20% and so on is used.

Bit error rate is the measure of performance of a digital communication system, which characterizes the reliability of the radio system through bits "in to out". The concept of bit error rate (BER) is simply given by,

BER = Errors/Total Number of Bits

Detection rate and false alarm rate of physical-layer channel authentication are two critical measurements. Detection rate of physical-layer channel authentication indicates the probability of illegal data frames detection and false alarm rate of physical-layer channel authentication denotes the probability of legitimate data frames detected as illegitimate. When the false alarm rate is smaller and detection rate is bigger, the authentication performance is better, where the false alarm rate of 0 and the detection rate of 1 are the ideal performances depicts the diagram of detection rate and false alarm rate of physical layer channel authentication for different adjusting parameter θ. The proposed scheme was compared with the performances of these schemes upgraded gradually with the increase of SNR, while the performance was better than those of the other schemes under the same SNR.

5.3 Discussions

After so many experimentation using MATLAB and SIMULINK we have arrived on conclusion that physical layer security is so important for wireless networks for many reasons discussed in this work, in addition it is un explored and new for the domain and potentially very rich on securing the channel using its unique features. We have used Beam forming and addition of noise in the medium so as to secure the channel while allowing the two legitimate users namely Alice and Bob to communicate while it is difficult for eavesdropper Eve to know the secret or unique physical layer secret, so Eve simply accept highly errored and degraded signal so that it can't decode it to a meaningful data, she could simply drop the data because it is meaning less and garbage.

The secret here is mainly on the knowledge of each other's channel state information of legitimate communicators, they know the other parties unique channel state information so that they can preprocess these information to use it on the steering in the process of steering matrix calculations, so that they use these to transmit the signal which is well mixed to hide it from the eavesdropper, in addition to this the signal is beam formed so that it is guided only to the direction of the intended user that every other directions luck the capacity to access the signal at least it is degraded in quality and strength to decode and recognize.

CHAPTER SIX

CONCLUSIONS AND FUTURE WORKS

6. 1 Conclusions

In this thesis work we try to see the vulnerability of wireless network to various types of attacks due to its broadcast nature and its use of air or radio frequency (RF) as a medium of communication that it is easier for eavesdropper to compromise the communication easily, so driven by this motive we exhaustively examine breaches of all types and come up with a solution for those issues discussed.

We propose a cross-layer secure physical-layer authentication framework for wireless network computing system with limited resources such as memory, processor and storage. The proposed scheme combines physical layer security PHY technology and traditional computational upper layer security the latter which is not a subject to this study because it is studied exhaustively, with physical-layer channel state information we can achieve mutual authentication between two intended terminal devices whereas unintended user is limited to not communicate because it lacks information about communication channels due to additional signal disruption of radio frequency using the introduction of noise to the channel and directional communication achieved between the two. Theoretical analysis and experimental results show that the proposed scheme can effectively boost the total success rate of access authentication and decrease the data frame loss rate to legitimate users while it increase data loss to unauthorized user significantly. It is not only highly secure due to higher secrecy but it is also simple and flexible, especially independent of a trusted party. In addition, the scheme could resist spoofing attacks, replay attacks, exhaustive attacks, and guessing and brute force attacks. It can significantly reduce the access authentication complexity and achieve greater security for any wireless system especially for low resourced sensors which can’t process high computational security through complex computation which needs high computing hardware with a higher resources like processor and RAM. Therefore, the proposed solution is very suitable for all resourced wireless network systems scenarios.

It is also useful for private key cryptography secret key exchange problem, it can exchange keys securely so that no one can intercept and steal, even as this framework is designed for multilayer security which incorporates cryptography by combining them all together therefore private key is safer when exchanged between two legitimate parities to start communication.

This thesis work contribute significantly to the journey of Physical layer security in such a way that it shows how it is possible to attain secrecy in Physical layer which is highly difficult to compromise for eavesdropper due to the benefit summarized as follows

- Bit error rate (BER) of the transmitted data is minimum or insignificant for intended user while it has a high BER for eavesdropper though it is received it is meaning less
- Since the channel is so secure it can also be used for cryptographic security as a private key exchange mechanism
- It is impossible for eavesdropper to guess or try physical layer channel state information since it is unique
- Physical layer security uses no computation like cryptographic security that it is appropriate for small devises like sensors, actuators etc.

6. 2 Future Works

We have been testing this physical layer security using Alice, Bob and Eve scenario of two legitimate communicator with eavesdropper Eve just to show how the system works for the scenarios presented, what needs to be done in the future is propagating this test work on the bulk to do that what it needs is high capacity computer and USRP devices designed to be tested in real environment with MATLAB itself, and then modelling and designing the Hardware and or the software driver based on these framework, this work is left for future.

The other future work for this thesis includes a MIMO transmission and reception by involving multiple antennas. By this concept in MIMO systems, the information could be transmitted more securely without any interception of an eavesdropper if any more in number. And integrating this Physical Layer Security to the upper layer computational security is left to future work though it is not as such difficult to deal with it.

References

[1] Junqing Zhang, Trung Q. Duong, Alan Marshall, and Roger Woods, “Key Generation from Wireless Channels" A Review; 2016.

[2] S. Gopalakrishnan, “A Survey of Wireless Network Security”, IJCSMC, Vol. 3, Issue. 1, January 2014, pg.53 – 68, ISSN 2320–088X.

[3] V. Bhujade, Deepak Chaudhary and Suraj V. Raut “A Survey on Basics of Cryptography” *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 6, Issue 3, March 2017.

[4] Jiazi Liu, "Novel Physical Layer Authentication Techniques for Secure Wireless Communications" Electronic Thesis and Dissertation Repository; 2015, Available: https://ir.lib.uwo.ca/etd/2794. [Accessed: September. 11, 2018]

[5] Surabhi Surendra Tambe, **“**WIRELESS TECHNOLOGY IN NETWORKS”; *International Journal of Scientific and Research Publications* , Volume 5, Issue 7, July 2015 1 ISSN 2250-3153 www.ijsrp.org. [Accessed: May. 20, 2019].

[6] S. Gopalakrishnan, “A Survay of Wireless Network Security”; *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.1 pg. 53-68, January- 2014.

[7] Murugiah Souppaya and Karen Scarfone, “Guidelines for Securing Wireless Local Area Networks (WLANs)” Recommendations of the *National Institute of Standards and Technology;; NIST Special Publication* 800-153; 2012.

[8] Rucher Bhatnagar and Vineet Kumar Birla, “WI-FI Security: A Literature of Security in Wireless network” *Research Scholar & Department of CSE & Mewar University*, India 2015.

[9] YI-SHENG SHIU AND SHIH YU CHANG, HSIAO-CHUN WU, SCOTT C.-H. HUANG, HSIAO-HWA CHEN, “Physical Layer Security in wireless Networks a tutorial”, IEEE Wireless Communications • April 2011.

[10] IEEE, “Signal Processing for Wireless Network Security” *Signal Processing Society* , Available: http://2018.ieeeglobalsip.org, November 26-28, 2018 [Accessed: Jan. 20, 2019].

[11] Jae-Jung Kim and Seng-Phil Hong, “A Method of Risk Assessment for Multi-Factor Authentication”, Journal of Information Processing Systems, Vol.7, No.1, March 2011 DOI: 10.3745/JIPS.2011.7.1.187.

[12] Hao Li, “Physical-Layer Security Enhancement in Wireless Communication Systems*”* the University of Western, Ontario, 2013.

[13] Dan Ekström "Securing a wireless local area network using standard security techniques", Master Thesis in Software Engineering Thesis no: MSE-2003:01 January 2003.

[14] D.Megala and Dr.V.Kathiresan, "Network Security Using Cryptography techniques" International Journal of Computer Application (2250-1797) Volume 7– No.2, March - April 2017.

[15] Abu Taha Zamani and Javed Ahmad "Wireless LAN Security: IEEE 802.11g & VPN", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 2, February 2014 ISSN: 2277 128X.

[16] Hawa Hoch Dirraneh and Hui Zhou, "Implementation of WLAN network with strong authentication" International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 10, October 2017.

[17] Anupriya Shrivastava and M A Rizvi, "Network Security Analysis Based on Authentication Techniques", Anupriya Shrivastava et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 11-18.

[18] Anjula Gupta and Navpreet Kaur, "Cryptography Algorithms A Review" Department of Computer Science, Volume 2, Issue 2 | ISSN: 2321-9939, 2014 Waliad

[19] Mounir Ghogho1 and Ananthram Swami, "Characterizing Physical-Layer Secrecy with Unknown Eavesdropper Locations and Channels", 2International University of Rabat, Morocco 3 Army Research Lab, USA, ICASSP 2011.

[20] Junqing Zhang and Trung Q. Duong, , Alan Marshall, and Roger Woods, "Key Generation from Wireless Channels: A Review" ACCESS.2016.2521718, IEEE Access

[21] Zhang, J., Duong, T. Q., Marshall, A., & Woods, R. "Key Generation from Wireless Channels: A Review," IEEE Access, 4, 614-626.https://doi.org/10.1109/ACCESS.2016.2521718.

[22] Frederick T. Sheldon "The insecurity of Wireless Networks" Oak Ridge National Laboratory, Copublished by the IEEE Computer and Reliability Societies, July/August 2012.

[23] Israa H. Latif and Ergun Erçelebi, "Implementation of Hybrid Cryptosystem using AES-256 and SHA-2 256 by LabVIEW", International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 6, Issue 1, January 2017.

[24] Yulong Zou, Jia Zhu, Xianbin Wang and Lajos Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", Proceedings of the IEEE Vol. 104, No. 9, September 2016.

[25] Kai Zeng, Kannan Govindan and Prasant Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks", Computer Science Department, University of California, Davis, CA 95616 {kzeng, gkannan, prasant}@cs.ucdavis.edu.

[26] https://www.mathworks.com/tagteam/87336_80780v00_Wireless_Design_Todays_ MATLAB_v2.pdf.

[27] Gunjan Verma and Paul Yu, “A MATLAB Library for Rapid Prototyping of Wireless Communications Algorithms with the Universal Software Radio Peripheral (USRP) Radio Family”, Army Research Laboratory, June 2013.

[28] Anupriya Shrivastava and M A Rizvi, “Network Security Analysis Based on Authentication Techniques” Department of computer engineering and application, NITTTR, Bhopal, India International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 11-18, ISSN 2320–088X.

[29] Jae-Jung Kim and Seng-Phil Hong, “A Method of Risk Assessment for Multi-Factor Authentication”, Journal of Information Processing Systems, Vol.7, No.1, March 2011 DOI: 10.3745/JIPS.2011.7.1.187.

[30] H. Vincent Poor and Rafael F. Schaefer, “Wireless physical layer security”, Department of Electrical Engineering and Computer Science, Technische Universit ¨ at Berlin, 10587 Berlin, Germany, 2016.

[31] Vijay Vaishnavi, Bill KuechlerStacie Petter and Gerard De Leoz, “Design Science research in Information Systems”, December 20 2017, url, Available: http://www.desrist.org/design-research-in-information-systems/, [Accessed: Jan. 12, 2019].

[32] “Theoretical framework”, Available: https://www.google.com/search?what+is+a+framework [Accessed: Nov. 12, 2018].

[33] “IT security frameworks and standards”, Available: https://searchsecurity.techtarget.com/tip/IT-security-frameworks-and-standards-Choosing-the-right-one.

[34] Lifeng Sang and Anish Arora, “A Wireless Security Framework without Shared Secrets”, Department of Computer Science and Engineering, the Ohio State University, Columbus, Ohio, 43210, 2009.

[35] “Edge computing devices”, Available: https://www.google.com/search?q=edge+computing, [Accessed: Jan 12 2019]

[36] Mathworks “Transforming Wireless Design with MATLAB”, 2016 The MathWorks http://mathworks.com/trademarks

[37] International Journal of Advanced Research in Computer and Communication Engineering, “Security Analysis of Various Public Key Cryptosystems for Authentication and Key Agreement in Wireless Communication Network”, ISO 3297:2007 Certified Vol. 6, Issue 2, February 2017

Annex

Sample code for Alice, Bob and Eve physical layer security simulation in MATLAB.

```
alice_bob_channel = repelem(reshape((randn(1,N)+
randn(1,N)*1j)/sqrt(2),2,N/2),1,2);
alice_eve_channel = repelem(reshape((randn(1,N) +
randn(1,N)*1j)/sqrt(2),2,N/2),1,2);
% Create Noise for Alice to Bob and Alice to Eve channels
ALICE_BOB_NOISE = 10^(-EsNo_dB(idx)/20) * (randn(1,N)+randn(1,N)*1j)/sqrt(2);
ALICE_EVE_NOISE = 10^(-EsNo_dB(idx)/20) * (randn(1,N)+randn(1,N)*1j)/sqrt(2);
 % Beamformer (Transmitter-based beamforming to Bob)
 alice_bob_channel_eff = alice_bob_channel.*exp(1j*angle(alice_bob_channel));
 % Received signals
 bob_receive = sum(alice_bob_channel_eff.*s,1) + ALICE_BOB_NOISE;
 eve_receive = sum(alice_eve_channel.*s,1) + ALICE_EVE_NOISE;
 bob_receive_noAN = sum(alice_bob_channel_eff.*s_noAN,1) + ALICE_BOB_NOISE;
 eve_receive_noAN = sum(alice_eve_channel.*s_noAN,1) + ALICE_EVE_NOISE;
 eve_x_estimate(d) = 2;
 elseif 135 <= angle_eve(d) || -135 >= angle_eve(d)
 eve_x_estimate(d) = 0;
 else
 eve_x_estimate(d) = 1;
 end
 end
 eve_b_estimate = reshape(dec2bin(eve_x_estimate).',1,2 * N);
 % Symbol decisions (Eve no AN)
 angle_eve_noAN = 180/pi * angle(eve_s_estimate_noAN);
 eve_x_estimate_noAN = zeros(1, N);
 for d = 1:N
 if -45 <= angle_eve_noAN(d) && angle_eve_noAN(d) < 45
 eve_x_estimate_noAN(d) = 3;
 elseif 45 <= angle_eve_noAN(d) && angle_eve_noAN(d) < 135
 eve_x_estimate_noAN(d) = 2;
 elseif 135 <= angle_eve_noAN(d) || -135 >= angle_eve_noAN(d)
 eve_x_estimate_noAN(d) = 0;
 else
 eve_x_estimate_noAN(d) = 1;
 end
 end
 eve_b_estimate_noAN = reshape(dec2bin(eve_x_estimate_noAN).',1,2 * N);
 % Count estimation errors
 bob_err(idx) = size(find(b - bob_b_estimate),2);
 eve_err(idx) = size(find(b - eve_b_estimate),2);
 bob_err_noAN(idx) = size(find(b - bob_b_estimate_noAN),2);
 eve_err_noAN(idx) = size(find(b - eve_b_estimate_noAN),2);

 % Display elapsed time
tElapsed = toc(tStart);
end
% Simulation results
```

```
bob_BER = bob_err/(2 * N);
eve_BER = eve_err/(2 * N);
bob_BER_noAN = bob_err_noAN/(2 * N);
eve_BER_noAN = eve_err_noAN/(2 * N);
% Plot results
close all
figure
axis([-35 60 10^-6 1])
grid on
title('QPSK Bit Error Rate (BER) - Additional Noise (95%) and TBeamforming');
legend('Bob (nTx=2, nRx=1, Tx BF)','Eve (nTx=2, nRx=1, Tx BF)','Bob (nTx=2,
nRx=1, AN and Tx BF)','Eve (nTx=2, nRx=1, AN and Tx BF)');
xlabel('SNR (dB)');
ylabel('Bit Error Rate (BER)');
```