Republic of Iraq

Ministry of Higher Education and Scientific Research

University of Babylon

College of Information Technology

Department of Information Networks

A Proposed Enhancement System for Security in Cognitive Radio Networks

A Thesis

Submitted to the Council of the College of Information Technology for Postgraduate Studies of the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Information Technology - Information Networks

By

Doaa Kareem Jasim Saleh

Supervised by

Prof.Dr. Sattar B. Sadkhan

2021 A.D **1443 A.H**

بسم الله الرحمن الرحيم

(وَقُلْ رَبِّ زِدْنِي عِلْمًا)

صدق الله العلي العظيم

(طه : 114)

Supervisor Certification

I certify that this thesis was prepared under my supervision at the Department of Information Networks / College of Information Technology / University of Babylon, **by Doaa Kareem Jasim** as a partial fulfillment of the requirements for the degree of **Master in Information Technology**.

Signature:

Name: *Prof.Dr. Sattar B. Sadkhan*

Title: **Professor**

Date: / / 2021

The Head of the Department Certification

In view of the available recommendation, we forward this thesis for debate by the examining committee.

Signature:

Name: **Prof.Dr. Saad Talib Hasson**

Title: **Professor**

Date: / / 2021

Certification of the Examination Committee

We, the undersigned, certify that (**Doaa Kareem Jaism**) candidate for the degree of Master in Information Technology - Information Networks, has presented his thesis of the following title (A Proposed Enhancement System for Security in Cognitive Radio Networks) as it appears on the title page and front cover of the thesis that the said thesis is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on: (November 18, 2021).

Signature:

Name: Bayan Mahdi Sabbar

Title: professor

Date: / / 2021

(Chairman)

Signature:

Name: Suad Abdullelah Abdulhussein

Title: Assistant. Professor

Date: / / 2021

(Member)

Signature:

Name: Ahmed Hussain Radhi

Title: Assistant. Professor

Date: / / 2021

(Member)

Signature:

Name: Sattar Bader Sadkhan

Title: professor

Date: / / 2021

(**Member**) // Main Supervisor

Signature:

Name: Dr. Hussein Atiya Lafta

Title: Professor

Date: / / 2021

(Dean of Collage of Information Technology)

Declaration

hereby declare that this dissertation entitled " **A Proposed Enhancement System for Security in Cognitive Radio Networks**", submitted to University of Babylon in partial fulfillment of requirements for the degree of Master in Information Technology \ Information Networks, has not been submitted as an exercise for a similar degree at any other University. I also certify that this work described here is entirely my own except for experts and summaries whose source are appropriately cited in the references.

Signature:

Name: Doaa Kareem Jasim

Date: /   / 2021

Dedication

To the soul of **my dear father**, may God have mercy on him

To **my dear mother**, may God prolong her life

To those who encouraged me to continue my scientific career, my **brother Muhammad Kareem**

To all **my family members** who were the best support and encouragement

And to **everyone** who encouraged and helped me complete this work

Acknowledgments

I thank God Almighty and praise Him, for He is the Most Gracious and Most Merciful above all else. I thank Him for achieving what I aspire to.

It enabled me to complete a master's degree in information technology to join the University of Babylon

I extend my great thanks and appreciation to *Prof.Dr. Sattar B. Sadkhan*

for his good cooperation, as he provided me with what I needed

To him from sources and inquiries and was present step by step in order to complete this study.

Grateful thankfulness and warm gratitude also extend to Information Technology College by its dean, it is head of the Information Networks department, its staff, and all my colleagues for their great potential in learning and encouraging me through my B.S.C and M.S.C studies.

I would like to thank my colleague, Amir Samir, who helped me obtain the study's sources and references.

And thanks to **my brother Muhammad** for the beautiful patience he showed in continuing and following him with the steps to complete the study and he was present at every step

Abstract

Cognitive Radio (CR) technology has been developed to overcome the scarcity of spectrum due to the rapid development of wireless networks. Both authorized and unauthorized users can use spectrum with this technology. Spectrum is dynamically distributed in perceptual radio networks, thus increasing spectrum usage and increasing attacks, including eavesdropping. There are two types of eavesdropping attacks **the first type** is passive attacks; the attacker doesn't commit any changes to the intercepted information. The attacker just needs to observe the transmission. and **the second type** the active attack includes modification of the message and causes a huge amount of harm to the system and is accomplished by gaining physical control over the communication link to capture and insert transmission. Transmitted data are protected from eavesdropping attacks in two ways. The first way the primary user is protected from passive eavesdropping is by allowing only the secondary users to know to use empty channels; however, any external user who does not know, is considered an attacker, and they are not allowed to use the empty channel. The second method uses a chaotic encryption algorithm where messages are encrypted before sending.

This study is proposed to enhance the security of cognitive radio networks through the implementation of the first way the chaotic encryption algorithm is used to protect messages from an active eavesdropping attack because the main advantage is that the chaotic signal appears to unauthorized users as noise, and the chaotic signals are very sensitive to the starting conditions and the second way we can protect data transmitted from passive eavesdropping through that are allow secondary users who know them through their IP addresses to use the empty channels, but any external user over there does not have an IP address it is considered an attack, they are not allowed to use the empty channel. So the security of the cognitive radio network is one of the most focused and interesting topics.

List of figures

Table of Contents

List of tables

List of abbreviations

NO.	Abbreviation	Definition
1.	AN	Artificial Noise
2.	AODV	Ad-hoc On-demand Distance Vector
3.	AWGN	Additive White Gaussian Noise
4.	BER	Bit Error Rate
5.	CBC	Cipher Blocker Chaining
6.	CBS	Cognitive Base Station
7.	CCDA	Common Control Data Attack
8.	CCR	Chaotic Cognitive Radio
9.	CFBSs	Cognitive Femto Base Stations
10.	co-NOMA	cooperative Non-Orthogonal Multiple Access
11.	COOK	Chaos On-Off Keying
12.	COP	Connection Outage Probability
13.	CRN	Cognitive Radio Network
14.	CS	Costas Sequence
15.	CSI	Channel State Information
16.	CT	Cognitive Terminal
17.	CUs	Cognitive Users
18.	DC	Difference Convex
19.	DCF	Distributed Coordination Function
20.	DM	Directional Modulation
21.	DPC	Dirty Paper Coding
22.	DSA	Dynamic Spectrum Access
23.	ECB	Electronic Codebook
24.	EE	Energy Efficiency
25.	EMD	Empirical Mode Decomposition
26.	FCC	Federal Communications Commission

27.	FDA	Frequency Diverse Array
28.	FHSS	Frequency Hopping Spread Spectrum
29.	GPS	Global Positioning System
30.	ICSI	Instantaneous Channel State Information
31.	IMEI	International Mobile Equipment Identifier
32.	MAC	Media Access Control
33.	MDS	Misbehavior Detection System
34.	MIMO	Multiple-Input Multiple-Output
35.	MIMOME	Multiple-Input Multiple-Output Multiple Eavesdroppers
36.	OFDM	Orthogonal Frequency Division Multiplexing
37.	PBS	Primary Base Station
38.	PCF	Point Coordination Function
39.	PHY	Physical Layer
40.	PN	Pseudo-Noise
41.	Pus	Primary Users
42.	QoS	Quality-of-Service
43.	RF	Radio Frequency
44.	SDR	Software-Defined Radio
45.	SEEM	Secrecy Energy Efficiency Maximization
46.	SISO	Single-Input Single-Output
47.	SOP	Secrecy Outage Probability
48.	SR	Secrecy Rate
49.	SRM	Secrecy Rate Maximization
50.	SSCCR	Subcarrier-Shifting-based Chaotic Cognitive Radio

51.	SUs	Secondary Users
52.	WSNs	Wireless Sensor Networks

Chapter One

General Introduction

1.1 Introduction

To accomplish dynamic spectrum access, cognitive radios are employed as a technology to dynamically configure their transmission properties. There are two sorts of users in a cognitive radio network (CRN): primary and secondary. Traditional wireless users or licensed users having access to a certain licensed domain are referred to as primary users (PUs). Unlicensed users using cognitive radios, known as secondary users (SUs), can use channels that are currently unoccupied but must forego returning PU channels in order to continue broadcasting on other channels [1].

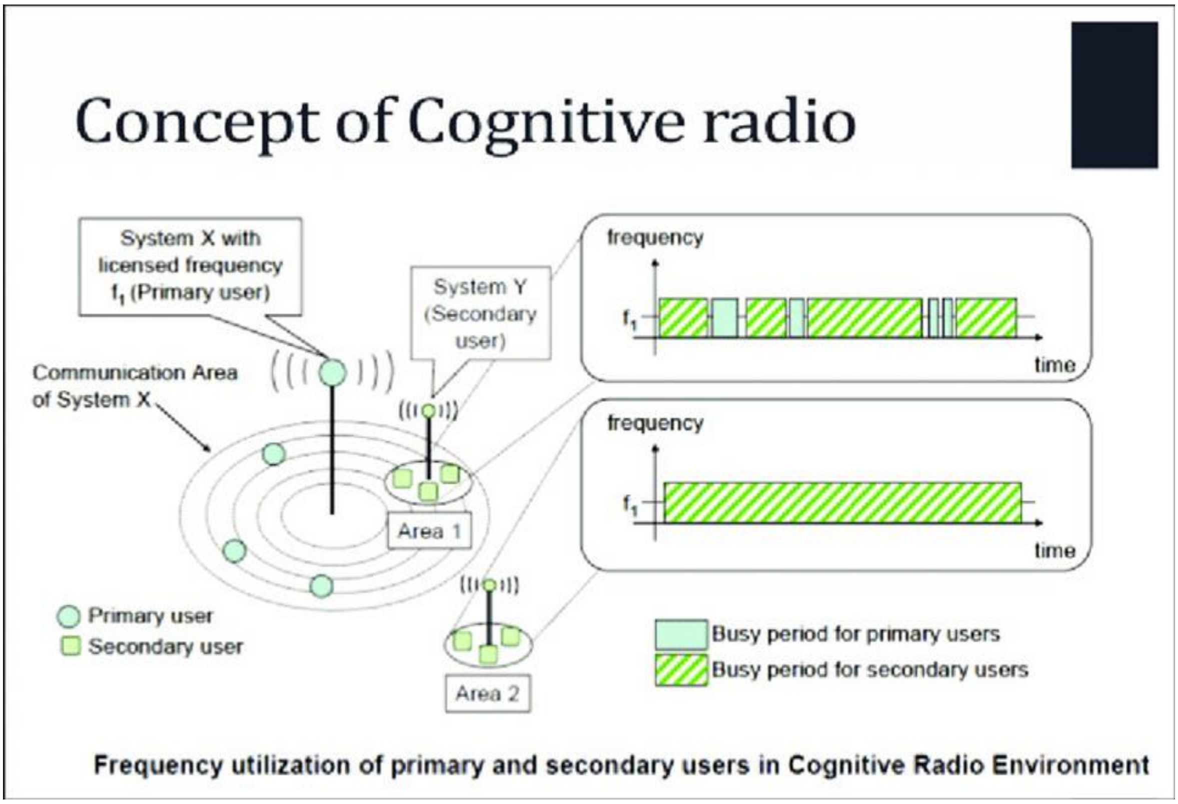
With the growing number of wireless networks competing for a limited radio spectrum, new issues have emerged. The traditional spectrum distribution is predicated on proper spectrum usage. However, it is stringent since each radio operator must have a license to operate on a certain frequency. More knowledge, blanks, and special energies in the radio spectrum are all on the agenda. To address this issue, technical resources have been devoted to improving spectrum usage in terms of the potential in order to have access to the dynamic spectrum. Detection of hidden networks of licensed spectrum zones without interfering [2].

Cognitive radio (CR) has become a promising technology for enhancing spectrum efficiency through adaptive reconfiguration of radio communication parameters in dynamically changing communication settings. At the same time, rapidly evolving technology has allowed software defined radio (SDR) platforms to have opportunistic access to radio spectrum to hardware to produce cognitive radio algorithms [3].

Cognitive radios are said to be one-of-a-kind, software-defined, artificially intelligent radios that can change operational parameters including frequency domains, modulation type, and power transmission without requiring hardware changes. Cognitive radios may actively search the available spectrum and dynamically adjust their operations to end their broadcast and avoid interference with existing users due to their characteristics [4].

After focusing on core operational challenges such as channel sensing, allocation, and management for several years, current cognitive radio research has shifted its focus to applications such as security [5].

When customers rely extensively on the transmission of important/private information over Wireless networks are used for credit card transactions and the exchange of banking data. As a result, being able to reliably divulge secret information in the presence of adversaries is critical. Opponents may undertake a variety of attacks to obtain unauthorized access to, alter, or even disrupt the flow of data [6]. The primary and secondary users must be secured because they share the same network. Without the usage of cognitive radios, they are more vulnerable to security assaults than traditional wireless networks. As a result, one of the most crucial aspects of criteria for CRNs is to provide strong security measures [7].



Concept of Cognitive radio

System X with licensed frequency f_1 (Primary user)
System Y (Secondary user)
Communication Area of System X
Area 1
Area 2
Primary user
Secondary user
frequency
f_1
time
frequency
f_1
time
Busy period for primary users
Busy period for secondary users

Frequency utilization of primary and secondary users in Cognitive Radio Environment

Figure (1.1) cognitive radio concept [68].

1.2 Problem Statement

Multiuser wireless network security is a major topic, Because of the opportunistic usage of licensed channels, CRN's open and dynamic features create a slew of additional security challenges and issues. Primary user emulation, objective functional attacks, learning attacks, data sensors, obfuscation attacks, and CRN physical layer eavesdropping are the six main types of attacks that have been known to occur [8].

There are two types of eavesdropping: passive and active. By passive eavesdropping, the hacker just "listens" to the data transmitted over the network while active can modify the transmitted. Figures (1.2) and (1.3) indicate variations between forms of eavesdropping. Unauthorized users may hear the intercept at the speed of the wireless link, making wireless communications particularly vulnerable to eavesdropping assaults. Security in physics layers is a realistic approach for securing the physical features of wireless channels that are used to protect wireless communications against assaults [9].

It is vital to safeguard the transmitted data. Traditional security methods such as network-layer encryption are being challenged by the growth of dynamic large-scale networks [10].

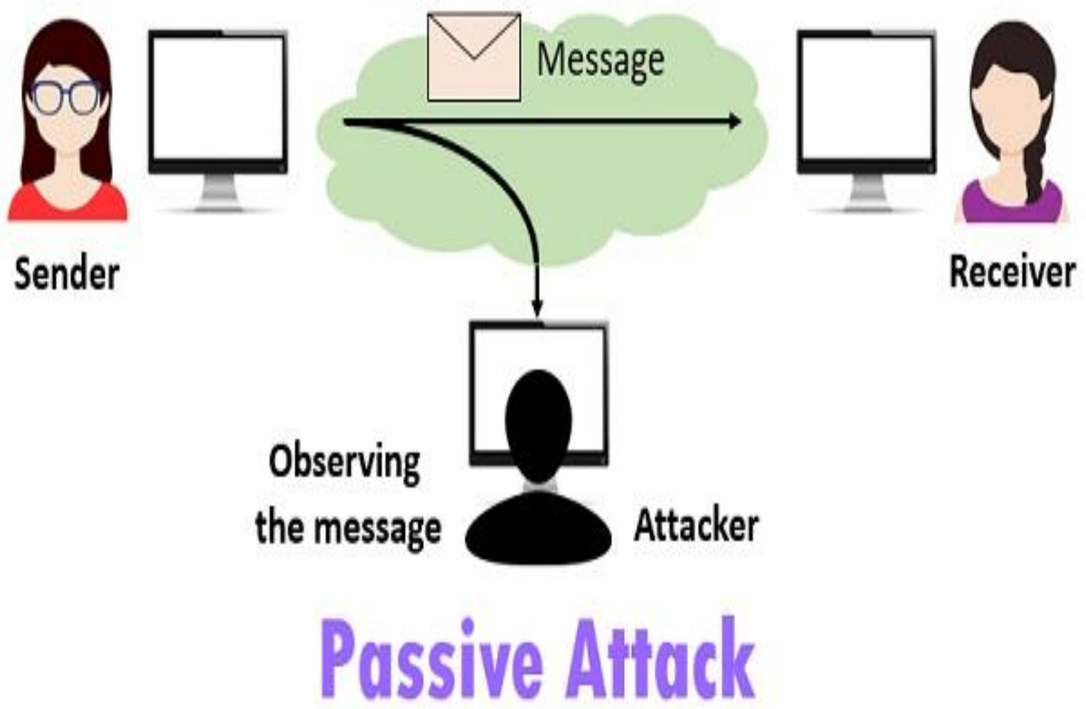


Figure (1.2) passive attack [69]

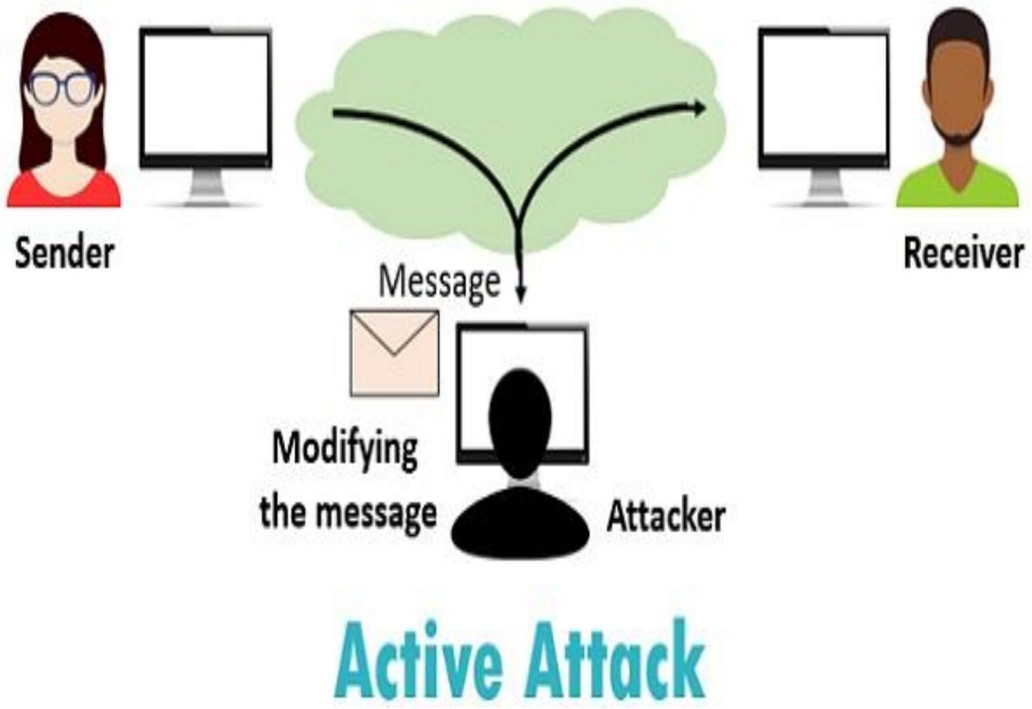


Figure (1.3) active attack [70]

1.3 Problem-solving methodology

Effectively defended against eavesdropping attacks in two ways. the first way the primary user is protected from passive eavesdropping attacks by allowing only secondary users they know to use empty channels done through giving secondary users IP addresses; However, any external user who does not know and does not have IP addresses is considered an attack, and they are not allowed to use the empty channel; The second way uses a chaotic encryption algorithm where messages are encrypted before sending.

In this instance, a chaotic encryption solution may be the best alternative. The chaotic signal appears to unauthorized users as noise, and chaotic signal sensitivity to start conditions, which allows starting states and control parameters as keys in the encryption procedure to be successfully used. In addition, the cost of generating a mess is really low [11].

1.4 The Aim of the study

This study is proposed to enhance the security of cognitive radio networks through implementation of: -

1- The chaotic encryption algorithm is used to protect messages from an active eavesdropping attack because the main advantage is that the chaotic signal appears to unauthorized users as noise, and the chaotic signals are very sensitive to the starting conditions

2- We can protect data transmitted from passive eavesdropping through that are allow secondary users who know them through their IP addresses to use the empty channels, but any external user over there does not have an IP address it is considered an attack, they are not allowed to use the empty channel.

1.5 Related Works

The research [12], created a traceable test framework for the assessment of dependability and safety in CRNs, where both the base station (BS) and the powerful primary user (PU) transmit secret messages to many evenly distributed PU in the presence of a random external intruder. A mobile correlation technique is used to reduce interference with PUs induced by Femto cognitive base stations (CFBSs). In addition, an eavesdropping area was created surrounding the BS to improve the confidentiality of the underlying networks.

In [13], the authors investigated the power distribution of base (PBS) and knowledge base transmitted via orthogonal frequency division multiplexing (OFDM) subcontractors in OFDM perceptual radio networks in the presence of a multi-antenna listening device. Artificial noise is used to mislead the eavesdropper at the cost of additional energy use in order to protect against eavesdropping. With the aim of improving the energy efficiency (EE) of secure communications, they propose a covert energy efficiency maximization scheme (SEEM) by making use of instantaneous channel state (ICSI's) information from an eavesdropper known as microinjection-based SEEM. (ICSI-SEEM). When ICSI is enabled, the eavesdropper ICSI additionally introduces a SEEM scheme through the use of Statistical CSI eavesdropping (SCSI), termed SCSI-based SEEM (SCSI-SEEM). Since ICSI-SEEM and SCSI-SEEM problems are both fractional and non-convex, they are first converted into comparable subtraction problems, and using the biconvex function approximation approach, approximate convex problems are accomplished. Finally, new two-stage algorithms are proposed in order to obtain optimal solutions because they have specific problem areas ICSI-SEEM and SCSI-SEEM.

The trade-off between reliability and safety is examined in the paper [14], which takes into account the maximum transmission power, interference strength, signal jamming, and Rayleigh fading, as well as our interference as an undistributed Gaussian parameter. To achieve this goal, the explicit closed formulas for the chance of rapid detection and the chance of successful eavesdropping were developed were first proposed and then confirmed using Monte Carlo simulations.

The objective of the paper [15], was introducing a cognitive safety (CS) approach to the physical layer of wireless communication systems to address wireless security issues throughout life. By merging adaptive security solutions into communication systems and exploiting the safety of physical layers from a fresh perspective, the technology provided would give entire safety to assure strong and dependable communication in the presence of opponents. Addiction results from modifying the dispersion qualities of the signal so that specific scenarios like user density, application-specific adaptation, and location within the CS concept provide a secure connection.

The paper [16] investigated a secure communication model for perceptual multi-user, multi-output, large-input (MIMO) systems with underlying spectrum sharing. Within a multiuser (licensed) MIMO platform, the primary spectrum sharing system is used to operate a large multiuser secondary (cognitive) MIMO system. Primary or secondary covert signals are considered to be eavesdropped on by a passive multi-antenna listening device. Synthetic noise generation (AN) in the primary base station (PBS) and no-effect pre-encoders are used to provide a physical layer security method for primary and secondary transmissions.

Using Poisson point operations and randomizing primary users, secondary users, and eavesdroppers, the authors of the paper [17] examined the architecture of secure transmission in random cognitive radio networks. By combining a secrecy protection zone with artificial noise, the authors present a simple and decentralized secure transmission technique based on this situation. This transmission strategy, in particular, helps improve confidentiality performance by distinguishing secondary transmitters based on the eavesdropping environment. They then check the performance of the secondary network outage and confidentiality outage; From which they derive the term closed speed data transfer. By determining the best transmission power for secondary's and the suitable power distribution between the information-carrying signal and spurious noise, they also discover how to optimize secondary network confidentially throughput under primary and secondary outages.

The physical layer security of a multi-input, multi-output bidirectional relay channel has been investigated in the paper [18]. Bob talked with the lawful destination point (Alice) via a bidirectional access point if there is a cooperative bidirectional jammer and probable eavesdropping (Eve). It's assumed that the cooperative jammer is the two-way node that operates only with radio frequency signals in the environment. They look at recycling the self-energy of the cooperative jammer and come up with a case that allows it to function as a node with a reliable power source.

They investigated the challenge of This document contains the pre-secret encoding of the cognitive eavesdropping system of MIMOME (Multiple Input and Multiple Output) [19]. The problem investigated through a pre-encoding approach using artificial noise (AN). This is followed by creating a secrecy rate maximization (SRM) problem, which is constrained both by interference power constraints imposed to protect the principal user (PU) as well as maximum transmission power for secondary transmitters. It was also decided to delete and revise the empty space limit from SRM issue. As naturally formed SRM problems produce differential convex (DC) programming issues, they answer them by using the following approach of convex approximation (SCA), where the non-convex components of each problem are approx. SRM issues can therefore be addressed repeatedly by successively programming their convex variants.

In the paper [20], an energy detector based on the experimental decomposition (EMD) procedure in unoccupied channels (dominant noise) is presented. To occupy a certain range of interest, the energy directly from the EMD signal processing is used. Performance is checked for different sound levels and sample dimensions of the proposed EMD-based detector. In addition, a comparison of the efficacy of the proposed detector is made using conventional spectroscopic sensing techniques, with the results showing that it exceeds other detection methods.

They explored the dynamic coordination of anti-eavesdropping project subcarriers in the paper [21]. The project deals with data protection between the transmission end and the legally acquired end. OFDM channel is used to send data from one place to another. This is an orthogonal frequency channel. The illegal extraction of data from a communication channel was carried out by eavesdropping at a third site. The phase of a given subcarrier can be calculated from the channel status information in real-time (CSI). Interference is done on the transmitter end in a deliberate manner to avoid eavesdropping.

An analysis of the time-domain AN generation mechanism for OFDM systems is presented in the study [22]. The time-domain AN generating mechanism is initially introduced for OFDM single-output (SISO) systems. A large number of antennas and longer periodic prefixes are required for standard time-domain AN generation in MIMO-OFDM systems (CP). As a solution to the problem, they provide another method of producing time ranges that While our proposed time-AN domains cancel out in the frequency domain, traditional time-AN domains do not.

They gave a summary of recent improvements in CR transceiver hardware design and algorithms in this paper [23]. UWB antennas and UWB antennas with reconfigurable bandwidths frequency/frequency adjustable antennae are the three types of antennas covered in the RF section. The primary design issues for the remaining RF blocks are also covered. The authors have a focus on complicated spectrum sensing algorithms that address challenges including model uncertainty, hardware restrictions, and broadband sensing.

A software-defined CRRM design presented paper [24]. This software-defined architecture can adapt to different connectivity models in LTE-A/LTE-B with correct settings and in terms of transmission reliability, it of QoS guarantees via optimum design control. By supporting a variety of CRRM schemes, this design greatly simplifies system implementation, allowing CRRM to move to the next level of development for the fifth generation (5G) cellular network.

When an eavesdropper is present, [25] they investigated a cognitive radio network with a single knowledge base station (CBS) and several cognitive users (CUs). When a spectrum gap is detected, CBS communicates with the (CUs) via the RCN's observed spectrum hole. An eavesdropper can hear the cognitive transfer between CBS and CUs since radio transmissions are aired. The eavesdropper attempts to understand the audible signals for intercepting reasons. They propose a multi-user scheduling approach for CBS cognitive transfers, which selects a CBS instantaneous maximum capacity controller that will interact with CBS to successfully fight an eavesdropping attack.

The article [26] provided an overview of CRs as well as its problems, with an emphasis on the radio frequency (RF) component. It highlights the current state of the associated regulatory and standardization processes, which are critical to the success of any emerging technology. They highlight several key research problems, particularly those related to cognitive radio (CR) dissemination. The focus is on RF front-end, transceiver, analog-to-digital, and digital-to-analog interfaces as they remain the major bottleneck in CRs development.

The paper [27], provided a thorough examination of the security and privacy concerns that arise in CWSNs by highlighting the many security risks that these networks face as well as the different defense techniques that may be used to mitigate these flaws. Various sorts of CWSN assaults are classified into distinct groups depending on their natures and targets, and relevant security procedures are presented for each attack class. In addition, certain significant research concerns in CWSN security and privacy are mentioned.

The work [28] provided a state-of-the-art summary of cooperative sensing in order to answer concerns about cooperative technique, cooperative gain, and cooperative overhead. The cooperative sensing method is investigated using cooperative sensing features such as cooperation models, sensing methodologies, hypothesis testing, data fusion, control channel and reporting, user selection, and knowledge base. In addition, the variables that influence the amount of cooperative benefit that may be achieved and the amount of cooperative overhead that can be spent are discussed. In cooperation, there are also open research challenges relating to each problem.

Secure information transfer was considered without knowing the eavesdropping channels or locations in wireless networks. in the paper [29], There are two main mechanisms: the artificial manufacture of noise the non-sender and recipient system contract; The variety of users that enables the receipt of messages when there is artificial noise. They establish the greatest number of eavesdroppers that may be separately running and distributed evenly while the requisite secrecy is attained with high probability within the limit of many system nodes.

In order to receive M-related data on the transmissions, the target users are separated into M groups in a multicast communication scenario, while the eavesdroppers (Eves) group attempts to intercept. In the paper [30], they propose directional modulation (DM), artificial noise (AN), matrix-aided Costas sequence (CS), and matrix frequency diverse array (FDA) in multicast precoding systems since wireless security systems include authentication and secure transmission.

A novel subcarrier switching-based Chaotic Cognitive Radio (SSCCR) approach has been developed in the paper [31] to boost the security of CCR systems. By combining the chaotic subcarrier sequence with the available subcarriers, they suggest transmitting information using a chaotic subcarrier pair. The subcarrier pairs would alter dynamically as the subcarriers changed. Another messy sequence defines a subcarrier conversion rule for security reasons. They obtain the bit error rate (BER) equation analytically using the adopted mathematical model.

When it comes to non-contiguous spectrum access, a chaotic cognitive radio (CCR) system offered the advantages of a chaotic communication system combined with the flexibility of a superposition cognitive radio (CR) system, according to the researchers. Rather than generating a chaotic sequence in the time domain, the proposed CCR system generates it in the frequency domain, allowing for non-con [32] They created bit-error-rate structures for CCR systems using additive white Gaussian noise (AWGN) channels as well as Rayleigh, Ritchie and Nakagami slow fading channels in this research. As a result of the probability distribution in a chaotic map, it is possible to analyze the transmitted signal energy distribution on the detected non-continuous sub-card bands and estimate a bit error level.

By offering a unique methodology for separating and detecting chaos from noise, this research [33] aimed to provide a practical solution to this challenge. Dynamical systems, imputation theory, matrix algebra, and statistical theory are all used in the proposed technique. The distribution, pattern, and behavior of subjective values are studied in depth to achieve their goal. This generates a number of useful qualities, including the ability to distinguish.

The criteria for an effective communication method for wireless sensing applications were examined. Chaos on-off keying (COOK), a no coherent direct chaotic communication technique, has emerged as a possible contender. To increase performance in noisy and fading situations, this research [34], presented a modified version of the COOK system. The suggested technique uses the idea of differential correlation to expand the signal space of the choice variable while keeping implementation requirements low.

Table (1-1) Shows the purpose of the previous works in the concept of the cognitive radio networks.

Number of References	The main aim	challenges	Status
[12] (2019)	This study proposes a traceable analysis approach for evaluating the reliability and security performance of cooperative non-orthogonal multiple access (co-NOMA).	The presence of randomly located external eavesdroppers-	A mobile association technique is used to limit the interference to PUs caused by cognitive Femto base stations (CFBSs). In addition, an eavesdropper-exclusion zone is established surrounding the PBS to improve the core networks' secrecy performance.
[13] (2018)	Artificial noise is employed to mislead the eavesdropper at the expense of additional power usage in order to protect against eavesdropping. With a view to improving the energy efficiency of secured communications (EE),	The existence of an eavesdropper has multiple antennas.	Artificial noise
[14] (2018)	Unlicensed users (UUs) and licensed users (LUs) can coexist in cognitive radio networks (CRNs), therefore mutual interference between UUs and LUs isn't ignored or treated as a Gaussian distributed quantity. Additionally, jamming signals to purposefully interfere with eavesdroppers' signal reception is a	-	An exact closed-form definition of detection probability and eavesdropping probability is first presented and then proven using Monte-Carlo simulations

	viable solution for improving the security performance of CRNs.		
[15] (2017)	With the goal of offering a comprehensive solution to wireless security concerns, cognitive security (CS) approach for wireless communication systems in the physical layer is offered.	-	The adaptiveness relies on the fact that radio adapts its propagation characteristics to satisfy secure communication based on specific conditions which are given as user density, application-specific adaptation, and location within the CS concept.
[16] (2017)	The research examines a secured communication paradigm with basic spectrum sharing for perceptual, multi-user, multi-outgo (MIMO) systems.	A passive multi-antenna eavesdropper is assumed to be eavesdropping upon either the primary or secondary confidential transmissions.	Artificial noise (AN) generation at the primary base station (PBS) and zero-forcing precoders are used to implement a physical layer security method for primary and secondary transmissions. The precoders are built specifically utilizing channel estimates with pilot contamination.
[17] (2016)	Using Poisson point processes to randomly distribute primary users, secondary users, and eavesdroppers, the authors of this research investigate safe transmission design in random cognitive radio networks.	-	By combining the secrecy guard zone and artificial noise, the authors suggest a simple and decentralized secure transmission technique.
[18] (2016)	In this paper, The physical-layer security of a full-duplex multiple-input multiple-output relay channel is investigated.	The presence of a cooperative full-duplex jammer and a potential eavesdropper (Eve)	To safeguard legal transmissions, they suggest a precoded artificial noise insertion technique.

[19] (2015)	In this research, They investigate the challenge of secrecy precoding for a cognitive multiple-input multiple-output multiple-eavesdroppers (MIMOME) wiretap system.	Multiple-input multiple-output multiple-eavesdroppers (MIMOME)	The problem is studied with an artificial noise (AN)-aided precoding scheme.
[20] (2017)	Enhancing the performance of non-coherent spectrum sensors such as energy detectors.	-	In this paper, an energy detector based on the conduct of empirical mode decomposition (EMD) in the unoccupied canals is presented (noise-dominant).
[21] (2015)	In this paper, they explored Dynamic Subcarrier Coordination for Eavesdropping Prevention.	-	Using the properties of OFDM systems, an anti-eavesdropping the system has been developed using dynamic subcarrier coordinate interleaving.
[22] (2014)	Artificial noise (AN) is a physical layer security approach that can be used to achieve secure communication. AN is a noise signal that is purposely sent together with data transmissions from the transmitter. Because AN is generated to be canceled out at legitimate receivers, it can prevent eavesdroppers from listening in even if the transmitters are unaware of their presence.	That this technique requires a large number of antennas at the transmitter and/or a longer cyclic prefix (CP).	The time-domain AN generation methodology for MIMO orthogonal frequency division multiplexing (OFDM) systems.

[23] (2014)	In this paper, they give a summary of recent improvements in CR transceiver hardware design and algorithms.	The main challenges faced by the design of the other RF block.	They investigate unsupervised classification techniques as well as a proposed reinforcement learning (RL) algorithm for decision-making in CR networks.
[24] (2014)	They reveal a software-defined CRRM design in this paper.	-	In LTE-A/LTE-B cellular networks, new communication paradigms such as heterogeneous network (HetNet) architecture, device-to-device (D2D) communications, and coexistence with current wireless systems have been introduced.
[25] (2013)	The security and reliability benefits through multiuser scheduling.	-	They examine the proposed multiuser scheduling scheme's security-reliability trade-off performance for cognitive transmissions with imperfect spectrum sensing over Rayleigh fading channels, where security and reliability are measured in terms of intercept probability and outage probability, respectively.
[26] (2012)	CRS provides additional flexibility and offers improved efficiency to overall spectrum use.	Intelligence distribution and implementation, delay/protocol overhead, cross-layer design, security, sensing algorithms, and adaptable hardware design are all challenges.	This article, provides an overview of CRS as well as its problems, with an emphasis on the radio frequency (RF) component. They highlight the current state of associated regulatory and standardization processes,

[27] (2011)	This paper provides a thorough examination of the security and privacy concerns that arise in CWSNs by highlighting the many security risks that these networks face as well as the different defense techniques that may be used to mitigate these flaws.	That one of the major challenges in CR networks is to detect the presence of primary users' transmission since malicious secondary users can send false spectrum sensing information and mislead the spectrum sensing data fusion process to cause a collision, interference, and inefficient spectrum usage	Various sorts of CWSN assaults are classified into different groups depending on their natures and targets, and appropriate security procedures are presented for each attack class.
[28] (2011)	To mitigate the impact of these issues, cooperative spectrum sensing has been shown to be an effective method to improve detection performance by exploiting spatial diversity.	Modeling of cooperation overhead and Modeling of primary user cooperation	To address the concerns of cooperative technique, cooperative gain, and cooperative overhead, this work provides a state-of-the-art summary of the field.
[29] (2011)	The main motivation is considering eavesdroppers of unknown locations, they first consider the case where the path-loss is identical between all pairs of nodes.	-	In this study, the authors demonstrate the maximum number of eavesdroppers that can be independently running and distributed uniformly, while yet achieving the required secrecy with a high probability under the limit of many systems no.
[30] (2020)	wireless security systems authentication and secure transmission	-	The authors of this work suggest directional modulation, artificial noise, matrix-aided Costas sequence (CS), and matrix frequency diversity array

			(FDA) for multicast precoding systems.
[31] (2015)	Increasing the security of chaotic cognitive radio (CCR) systems.	-	In this paper, they introduce a new subcarrier-shifting-based chaotic cognitive radio (SSCCR) strategy
[32] (2015)	They look at the bit error rate (BER) performance of a chaotic cognitive radio (CCR) system, which combines the benefits of a chaotic communication system with the flexibility of an overlay cognitive radio (CR) system in non-contiguous spectrum access.	-	In this paper, they construct the bit error rate formulations of CCR systems for additive white Gaussian noise (AWGN) channels as well as slow flat Rayleigh channels.
[33] (2012)	To increase performance in noisy and fading situations, this research, presents a modified version of the COOK system.	-	The suggested technique uses the idea of differential correlation to expand the signal space of the choice variable while keeping implementation requirements low.
[34] (2004)	This paper, tackles the channel distortion problem and presents a strategy for channel equalization.	-	A modified neural recurrence (RNN) network with a special training (equalizing) method is used to perform the suggested equalization.

1.6 Outlines of Thesis

The remaining chapters of this thesis are organized as follows: **Chapter Two,** the security of cognitive radio networks that contain the key functions of CR networks are (1) spectrum sensing, (2) spectrum management and decision, (3) spectrum sharing, and (4) spectrum mobility, Cognitive radio architecture is made up of I,) Physical Layer, ii) MAC Layer, ii) Network Layer, and iv) Transport

Layer, as well as v) Applications, and contain architecture Infrastructure-based CRN, an ad-hoc radio cognitive system, and cognitive radio mesh networks may be characterized as CRN, and also present attacks of the physical layer, mechanism of defenses in CRNs, chaotic encryption and simulation tools used to enhance the security of cognitive radio network. **Chapter Three** presents the proposed system, explains the practical stages of the system, and explains the proposed algorithm system can use the chaotic encryption algorithm is used to protect messages from an active eavesdropping attack because the main advantage is that the chaotic signal appears to unauthorized users as noise, and the chaotic signals are very sensitive to the starting conditions. We can protect data transmitted from passive eavesdropping through that are allow secondary users who know them through their IP addresses to use the empty channels, but any external user over there does not have an IP address it is considered an attack, they are not allowed to use the empty channel. **Chapter Four** describes the results of the proposed system. **Chapter Five** presents the conclusions of the results. Also, it describes future suggestions.

Chapter Two

The Security of Cognitive Radio Networks

2.1 Introduction

The cognitive radio system was introduced as a handy technique for improving the utilization of radio spectrum in the next generation of wireless communication and tackling spectrum scarcity. It enables secondary/unauthorized users (SUs) to discover unoccupied primary communication channels, known as spectrum gaps, and use them to transmit data without interfering with primary/authorized users (PUs). When it comes to perceptual radio cycles, spectrum sensing is key [35].

The cognitive radio system is divided into three primary paradigms based on how it allows secondary users to utilize the Licensed Spectrum Band:

1. **Interweave networks: -** These work without causing interference and stick to the basic notion of using spectrum gaps (e.g., vacant or not fully utilized within a certain geographical area of slots and parts of the spectrum). The interweaving devices can start data transmission, as soon as a spectrum hole occurs, but must terminate their transmission when sensing algorithms resume. Such techniques include matching filter, geostationary, signal or value-based detection, and beacon sensing. Other systems employ off-band beacon emissions or databases for geolocation [36].
2. **Underlay networks: -** In these, transmission is simultaneous for PU and SU devices over the same slots of the spectrum. Therefore, it is not necessary to detect spectral gaps. The temperature of the PU receiver should be below the threshold. SUs may lower transmit power, cancel interference, and implement non-contact zones (Guardia regions) surrounding primary recipients in order to lower the interference temperature. These areas can be augmented with data from past locations from a central console via a geolocation database, GPS (Global Positioning System) [37].
3. **Overlay networks: -** They allow PU and SU to be sent simultaneously. However, the distinction between SU devices is that they should be aware of the data (i.e. message) encoding techniques that are conveyed by the PU (codebook). This information may be used in two ways. The employment of cancelation techniques, such as dirty paper coding (DPC), that precedes the sent data, to prevent interference can first be used to cancel PU interference on SU receivers. Secondly, SU nodes can be utilized to

collaborate with the main network through the transmission of PU messages [37].

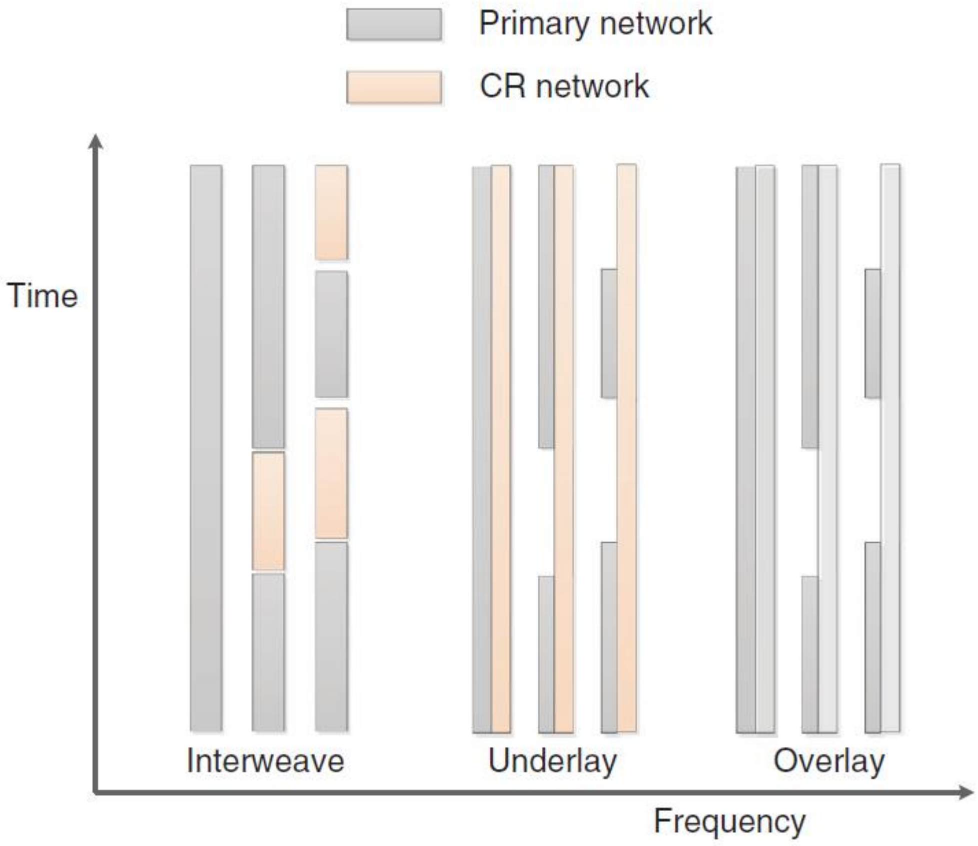


Figure (2.1) Interweave, underlay, and overlay modes of cognitive radio [39].

Since SUs must adaptively access the licensed spectrum, the CR networks need to enable additional features. To enable opportunistic spectrum access, the key functions of CR networks are (1) spectrum sensing, (2) spectrum management and decision, (3) spectrum sharing, and (4) spectrum mobility. These are briefly described next:

1) Spectrum sensing: Unused spectrum may be sensed by SUs and exploited without damaging PU functionality. The "spectrum hole" is a key need of CR networks. The most effective approach to identify a "spectrum hole" is to identify PUs. The methodologies of spectrum sensing can be categorized as three: (1) cooperative spectrum detection (several SUs share information on sensing with one other and include it for the identification of the PU), (2) interference-based detection, and (3) main transmitter detection [38].

2) Spectrum management: SUs capture the finest possible spectrum in order to satisfy communication needs while without interfering with other PUs harmfully. For the quality of service (QoS) criteria, CRs should decide on the optimal spectrum bands to fulfill the total available spectrum bands. These control operations can be characterized as 1) analysis of the spectrum and 2) spectrum choice [39].

3) Spectrum mobility: SUs vary their frequency of operation according to their radio environment. When using CR technology, SUs can function in the optimum frequency spectrum accessible while maintaining smooth communication demands during a transition to higher speeds, which is the goal of the technology. This results in a new sort of spectrum handoff, reference being made to the procedure determined by an SU and switched to a new available channel in order to keep the existing spectrum transmission going. Due to the moment when the spectrum transmission is carried out, there are two forms of spectrum mobility: (1) reactive and (2) pro-active [40].

4) Spectrum sharing: SUs offer a fair technique for programming the spectrum. Spectrum sharing is one of the biggest issues in open spectrum use. In the present wireless networks, it is considered a media access control (MAC) problem [41].

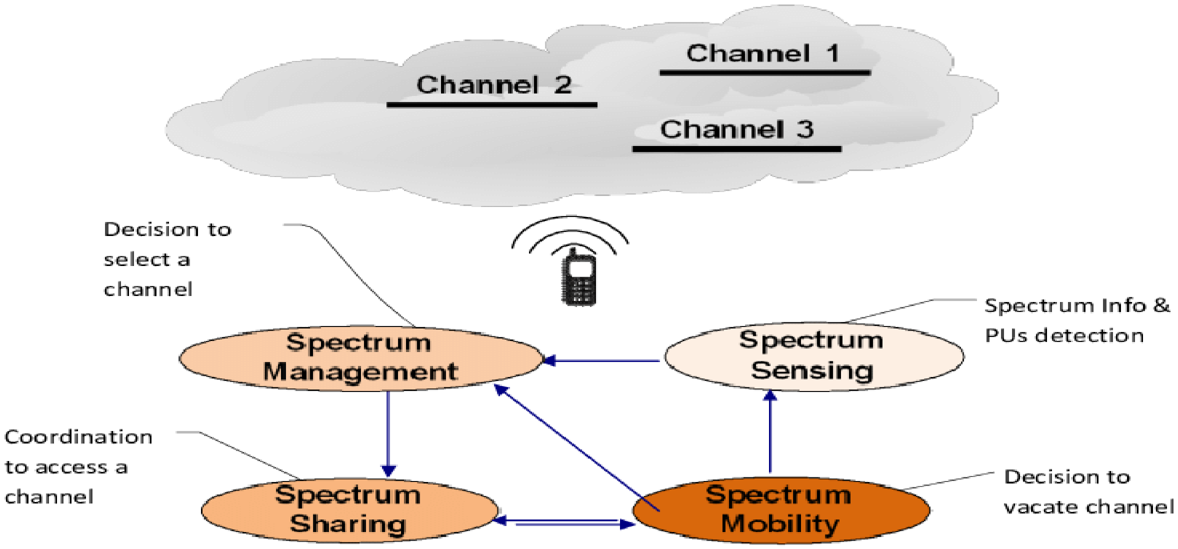

Channel 1
Channel 2
Channel 3
Decision to select a channel
Spectrum Info & PUs detection
Spectrum Management
Spectrum Sensing
Coordination to access a channel
Spectrum Sharing
Spectrum Mobility
Decision to vacate channel

Figure (2.2) the major functions for the CR networks [71].

2.2 Cognitive Radio Networks Architecture

Software-defined radio is the main hardware component of cognitive radio. The RF front end, a modem, and a receiver-transmitter chain are the main components of a software-defined radio.

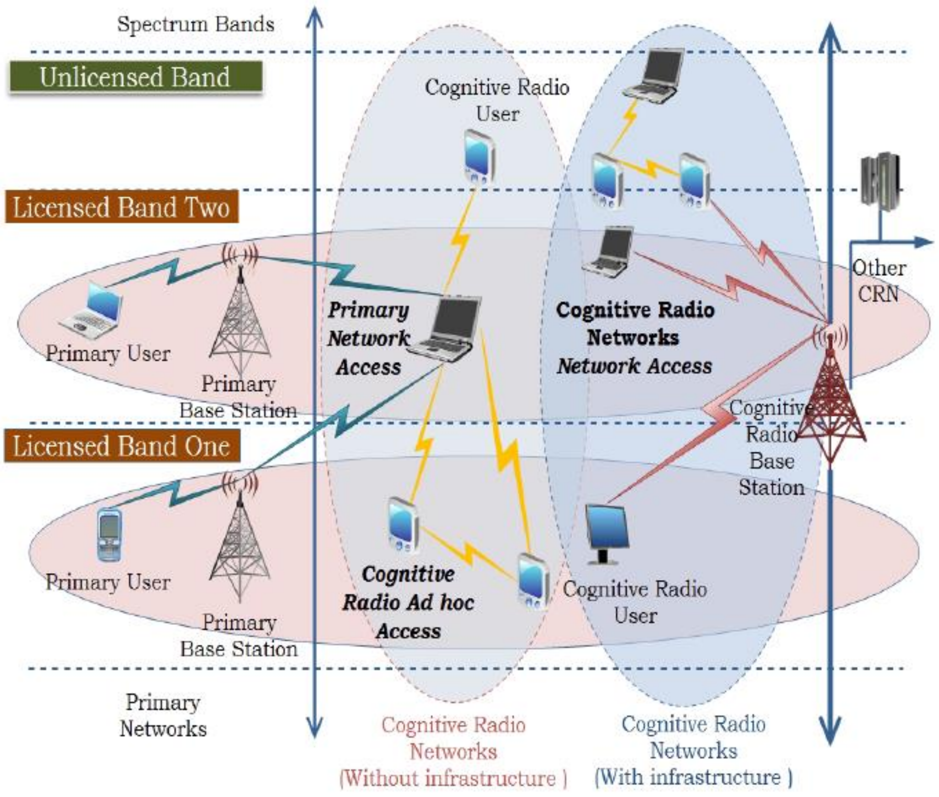


Figure (2.3) Cognitive Radio Architecture [43]

Cognitive radio architecture is made up of I,) Physical Layer, ii) MAC Layer, ii) Network Layer, and iv) Transport Layer, as well as v) Applications.

1)Physical Layer-: The main goal is the detection of spectral holes/opportunities in large frequency spectra and the measurement of opportunities and interference in the physical layer spectrum of primary receptors (eg, in a CDMA environment) [42].

2)MAC Layer-: As part of the MAC, a decision is made on whether or not to communicate faulty spectrum sensing information (such as what modulation and amount of power to use) and how to split the spectrum with other CRs into cases when the transmission is desired. As a result, it is recommended that the transmission processes. Information on spectrum sensing and spectrum access decision-making, synchronization of transmission parameters (for example, channel or time slot) between the transmitter and receiver, conciliation of spectrum allocation between primary and secondary users, and communication between secondary users are also included in the feasibility assessment of the MAC protocol (e.g., spectrum bidding and spectrum pricing) [42].

3) Network Layer-: Topology, addressing, and routing are the key duties of the network layer. Spectrum detection, neighbor finding, and topology maintenance are part of topology creation (e.g., through spectrum mobility) [42].

4)Transport Layer-: For flow and blot controls whose performance is impacted by MAC protocol performance and spectrum mobility, the transport layer protocol is responsible. The spectrum management approaches substantially influence transmission control protocol performance [42].

5) Applications Layer-: In the uppermost levels perform the execution of waveforms. The aim of the software architecture of an SDR is to standardize waveforms and apps on a software-based radio platform. These waveforms and apps are installed, operated, and replaced by other user-related apps. The hardware platform must be a highly standardized platform to standardize waveform and application interfaces [42].

The CRN architecture provides a framework that specifies the physical components and operations of the network. CRs can only connect with the base stations in a network-centered design (BSs). On the other hand, when these two nodes are on the same channel, communication between two nearby cognitive nodes can be established within a custom architecture. Since every node has a channel in its own cognitive ad hoc network, a link between 2 nodes must be made between at least one adjacent node in the accessible channel groups [43].

Infrastructure-based CRN, an ad-hoc radio cognitive system, and cognitive radio mesh networks may be characterized as CRN.

1)The infrastructure-based CRN: - This is a networking architecture in which cognitive terminal (CT)/cognitive radio (CR) and the base station (BS) are the core components of the design. CTs can only interface with BS in the infrastructure-based architecture (Fig. 2.4). Therefore, BS must be employed as an intermediary node if two CTs want to communicate between themselves. BS analyzes local CT spectrum observation data in the infrastructure-based CR networks and decides the use of spectrum [43].

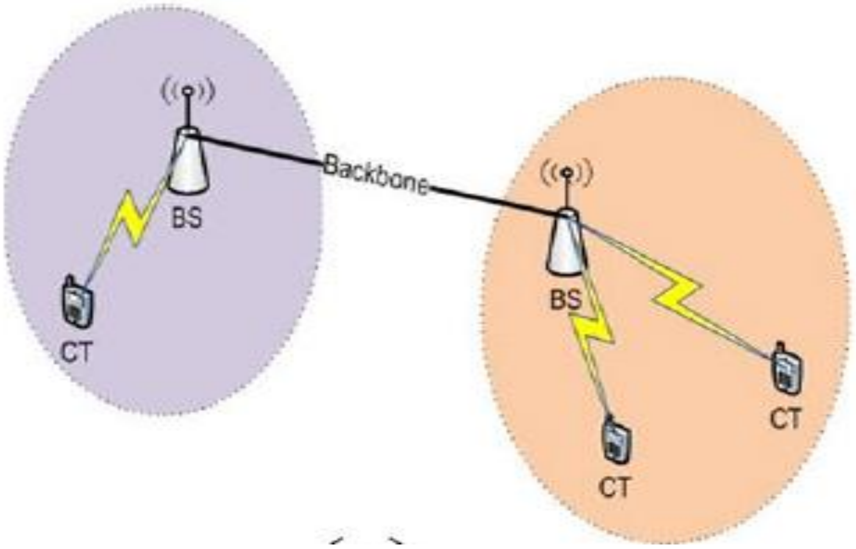


Figure (2.4) Infrastructure Architecture (single hop) [43]

2)The architecture of a CR ad hoc network: - As displayed in Figure (2.5), two sets of users may be divided: the main network component and the CR network component. The core network is made up of key users who have been granted permission to operate in a specific frequency band. The CR Network is made up of CR users who share wireless channels with other approved users of various bespoke applications [44].

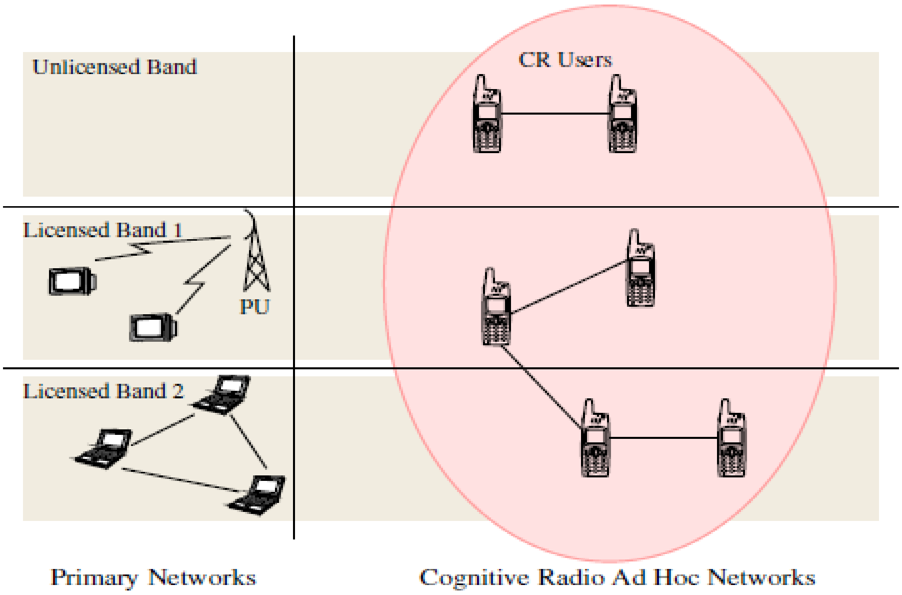


Figure (2.5) The CR ad hoc architecture [44]

3) Mesh CR networks: - Cognitive radio mesh networks blend in one of the CR and ad-hoc network infrastructure designs. It employs mesh topology in which several base stations create a single backbone (Fig. 2.6). A mesh CR network might easily resolve the difficulty of selecting routes and deciding on the spectrum. In different cognitive radio operations, medium access control plays a vital role, including spectrum mobility, spectra-sharing, assignment of resources, and sensing on the channels. If the main user is found, a secondary user has spectrum mobility to leave the channel and reach an idle channel, in which the communication link can be restored. Channel sensing enables a cognitive user to collect information about spectrum utilization and dynamically record available channels. According to the QoS needs, cognitive users are allotted accessible channels through the distribution of resources. Spectrum access is used to address disputes between diverse primary and secondary users to minimize detrimental interference. The initial step in developing MAC protocols for cognitive radio in unlicensed circumstances is the multi-channel MAC protocol for ad-hoc wireless networks. These protocols deal with similar problems; working in a multichannel setting and encountering the concealed terminal on several channels. However, more complex sensing functions may be used by cognitive radio to secure licensed broadcasts and distinguish between primary and secondary users. In a cognitive network, a variety of channels accessible for each user fluctuate with time and space, as opposed to a multi-channel network. Furthermore, the time scales are extremely different for cognitive radio and ad hoc radio. In the case of cognitive radio, secondary users must employ periodic sensing to understand the evolution of the wireless environment and users must swiftly modify their conduct to meet interferences. [45].

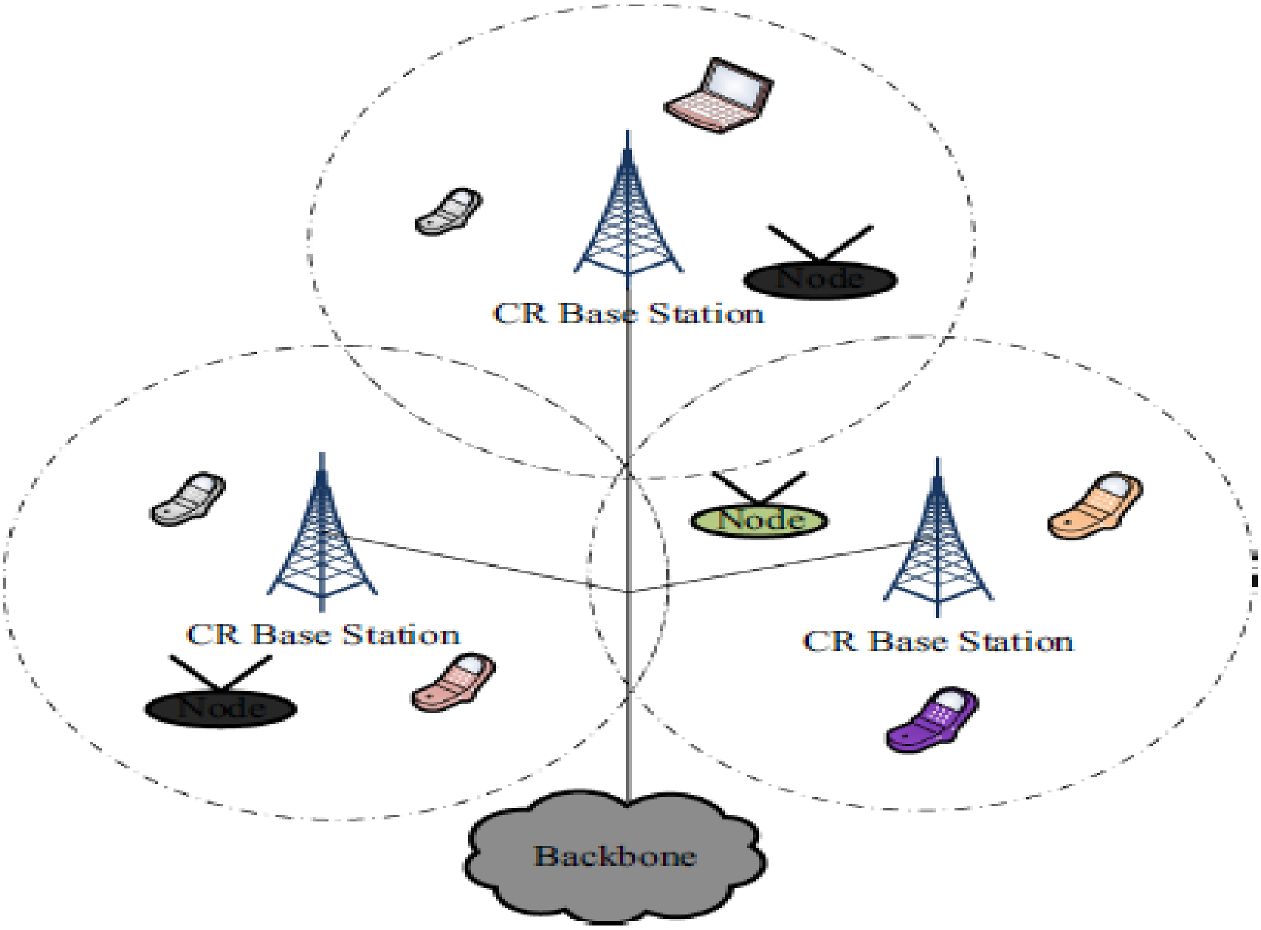


Figure (2.6) Mesh CR network architecture [45]

2.3 Security of Cognitive Radio Networks Benefits

Cognitive radio may be adapted to the surroundings and make modifications based on the capacity to communicate securely. The security is sensitive for the wireless network when compared with the wire network. If information is transmitted over a wireless network, jamming may be done, or it can be changed. The distinguishing property of cognitive radio networks is that safety is vital [46,47].

Because wireless media is transmitting, security is a major concern in wireless communications. Encryption technology has always been used to provide secure communication. However, if eavesdroppers have unbounded computing capacity, the cryptography's entire confidentiality cannot be guaranteed. Because network nodes are designed to be smarter, security considerations in CRNs are more complicated, and there is more attack potential than in traditional networks. To limit the risk of hostile nodes assaulting the CR network, security procedures and policies must be introduced. To offer a secure connection through wireless network nodes, confidentiality, integrity, availability, and authentication are only a few of the concepts that should be used. Protecting information from unauthorized disclosure to systems or individuals is referred to as confidentiality. Information confidentiality is required in wireless networks in general to preserve the privacy of the data owner, which may be a bank that holds a customer's credit and balance information [48].

2.4 Reliability

Reliability refers to the frequency with which a method measures and as long as the identical outcome can be achieved on a When it comes to reliability and stability, wireless networks are prone to interference from other networks, wireless-enabled devices, and impediments such as walls.

For wired networks, network dependability analysis has been a major subject of study for a long time, but not for Wireless networks, on the other hand, are being used in an expanding number of applications, offering mobile users complete and continuous access to computing resources, thanks to the advancement of mobile technology Unreliable wireless networks are more prone to failure because of a lack of transmission power or because of geography, interference, and other. As a result, wireless network reliability needs should be thoroughly evaluated. On the other hand, reliability for wireless networks differs greatly from that for wire networks, as wireless networks are uniquely functional and are known as terminal mobility, where the types and numbers of communication components change over time [49].

To recognize the initial signal accurately in a noisy and dim environment, and to neutralize unwanted users, cognitive radio networks face major challenges [50].

There is a growing demand for reliable, efficient security measures to protect content confidentiality and prevent unwanted access with the use of open networks and the Internet for multimedia data. The use of data encryption is one of the various options. Encryption schemes are methods that change data (such as text, image, sound, and so on) during transmission to make it unreadable, invisible, or impenetrable [49].

Data encryption is now widely used in a variety of applications, and numerous encryption techniques have been created with the purpose of protecting sensitive data by strengthening its security and confidentiality. In this respect, chaotic encryption can be the best option. The fundamental advantage is that the messy signal looks like noise to unauthorized users and that the messy signal is particularly sensitive to initial conditions which enable the initial states and control parameters in the encryption process to be used effectively as keys [50].

2.5 Attacks on Cognitive Radio Networks

The attack on cognitive networks is defined as an action that leads to (a) unacceptable interference with authorized main users or (b) missing secondary user chances. An assault is deemed to be powerful if there is a small number of opponents who do minimum operations but cause the primary and secondary users in the network maximal damage/loss. In this section, assaults on different cognitive network levels are described. Most of the attacks that we discuss leverage a dependability problem or problems. We examine the physical layer, link layer, network layer, transmission layer, and application layer in the Protocol Stack [51].

2.5.1. Physical Layer Attacks

For the effective deployment of CR systems, the development of enhanced physical layer transceivers is a crucial priority. The physical-level security (PHY) of the protocol stack in secure communication systems cannot be a replacement for cryptographic techniques. Threats to security may be brought about by passive nodes that attempt to intercept communication between authenticated nodes. In the process of crypto graphing techniques in protocol stacks, traditionally there were various indicators that cannot challenge [52].

1. Jamming Attack

When the jammer transmits a constant data packet to the channel, the SU never feels the channel is idle [53].

2. Primary User Emulation Attack

The decision procedure is not trustworthy if a CR is misled with incorrect information regarding the presence or absence of the principal user. Attackers make use of this notion and execute a main user emulation assault to fool users (PUEA). In this type of attack, the adversary node imitates the PU's transmission characteristics and behavior. This means that if any SU is subjected to this assault during the sensing phase, it recognizes the presence of the PU. As a result, even though the PU is not using the channel, the SU should leave it immediately. This attack is possible due to the lack of authentication procedures. PUEA can be performed on many channels by some attackers.SU thus works on all these channels, preventing them from being accessed [54].

3. Objective function attack

Cognitive radios can adapt to the environment. To adapt the radio to the environment by maximizing objective functions, and therefore to communicate with the radio through a medium, there are several radio settings that can be Goal assaults can be used against any learning system that makes use of goal-based Attacks of Faith Manipulation are a fancy way of The parameters handled include but are not limited to bandwidth, encryption, and channel access protocol [55].

4. Common control data attack(CCDA)

CCDA is a significant issue, which interferes with transmission by prohibiting channel elements from communicating spectrum information and also providing the attacker with all the information [53].

5. Eavesdropping Attack

That is a passive attacker and becomes undetected since the CR transmission is overheard by the eavesdropper without the emission of an active signal. In general, the use of secret key cryptography approaches to preserve secrecy from eavesdropping is introduced, however, the secret key management has resulted in an added system complexity. In addition, the secret major distribution is based on trustworthy infrastructure, which in certain situations may not be accessible or even corrupted. In order thereby to accomplish absolute secrecy against the theoretical exposure of data, the physical layer safety now emerges as a potential paradigm by using the physical properties of wireless networks. This has also a strong potential to combat the safety of CR communications Figure (2.7) An example of Eavesdropping Attack [56].

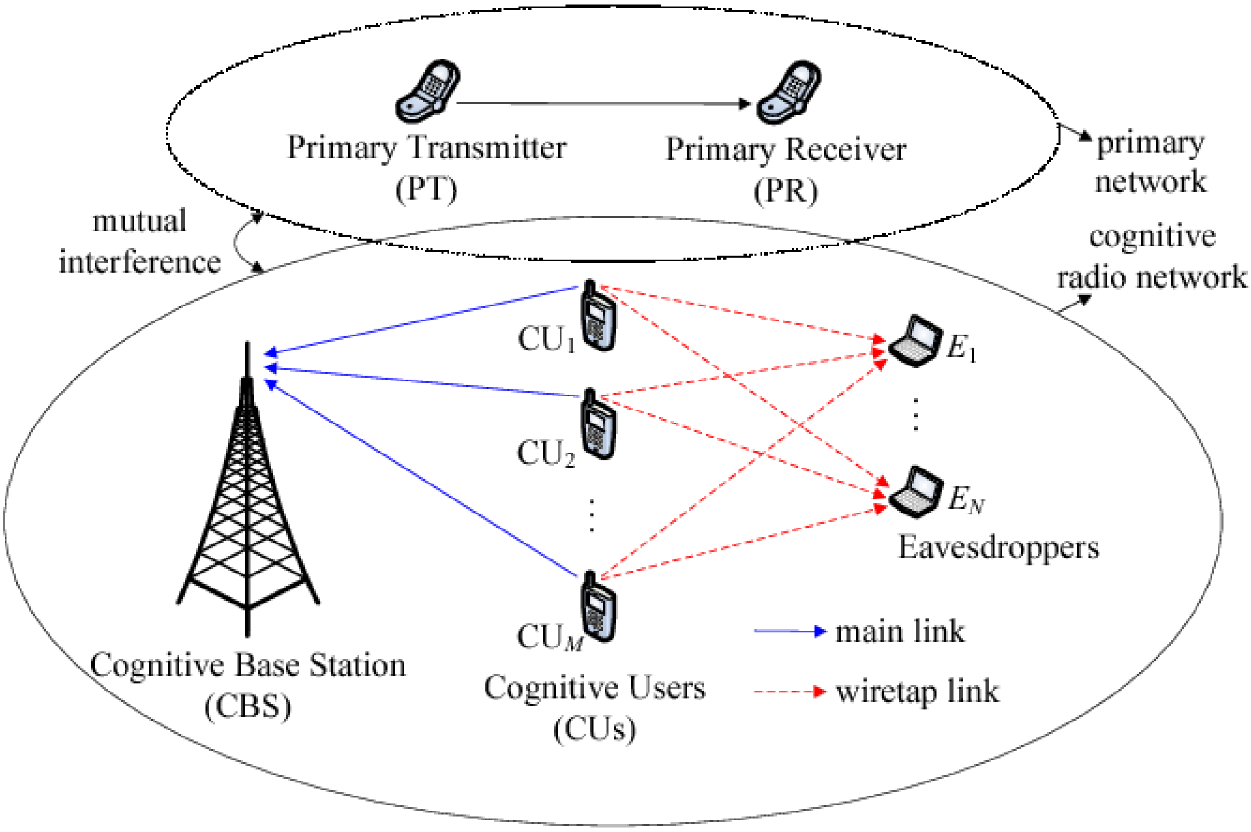


Figure (2.7) An example of Eavesdropping Attack [56]

2.6 Defenses Mechanism in CRNs

A number of investigators have taken efforts to address safety standards and ensure safe communication between SUs using various safeguards, such as authentication and authorization access through a variety of ways, within the CRN [53].

1. Digital Signature

Protect the integrity of message routing in hop-by-hop mode by use of a digital signature. This implies that every node signs its messages for routing, but no recipient can verify the source of routing information from the other nodes. A digital authentication system based on the signature, which is carried out in the physical and data link levels and allows trustworthy customer access to spectrum at CRNs. Although this work is important as a means of ensuring communication inside CRN, the performance evaluation reveals that the transmission of messages with a digital signature takes a long time compared to the regular transmission without a digital signature [57,58].

2. Trust-based Mechanisms

Mechanisms of trust have been proposed, (a) CRN reliable collaborative spectrum sensing, (b) the detection of unreliable hostile nodes, based on their reported history, against false alert and false alarm attacks, (c) detect suspect CUs, (d) defend against PUEA attacks, and (e). Nearly all CRN trusts are based on the general confidentiality or variation paradigm [53].

3. Timing parameter

In the MAC Layer, time parameters are proposed. During the negotiation phase, the node that receives the request establishes timing parameters to govern the time period. As a result, the sender is forced to transmit data at a slower pace. The receiver node takes action against the sender if the sender does not obey and transmits packets more often. The receiver node then examines the sender's actions and broadcasts the results over the current network [53].

4. Pinokio

Pinokio is a technique for detecting Byzantines. Pinokio employs a Misbehavior Detection System (MDS), Using training data to establish a typical behavior profile of the network. MDS identifies misconduct by observing bitrate behavior. The bit rate should regularly be altered and consistently altered by a node, the bit rate between two nodes should be mutual and the lower bit rate, according to the protocol, must be used over a small channel. Nodes that don't display these features aren't behaving in a way that promotes spectrum efficiency, thus they're questionable [53].

2.7 Chaotic Encryption

The rapid and increasing expansion of multimedia data interchange needs dependable and effective security measures to ensure content confidentiality and prevent unwanted access. The use of data encryption is one of the various options. Encryption schemes are methods that change data (such as text, picture, sound, and so on) during transmission to make it unreadable, invisible, or impenetrable. Data encryption is now widely used in a variety of applications, and different encryption systems have been created with the purpose of protecting sensitive data by strengthening its security and secrecy [61].

The majority of the study focuses on improving encryption quality, reducing execution time, and increasing security resilience against assaults. When compared to typical encryption systems, chaos-based systems have shown to be superior in terms of greater security and privacy due to the use of changeable keys. The basic idea is to employ a variety of chaotic components to enhance a scheme's confusion and dispersion abilities [61].

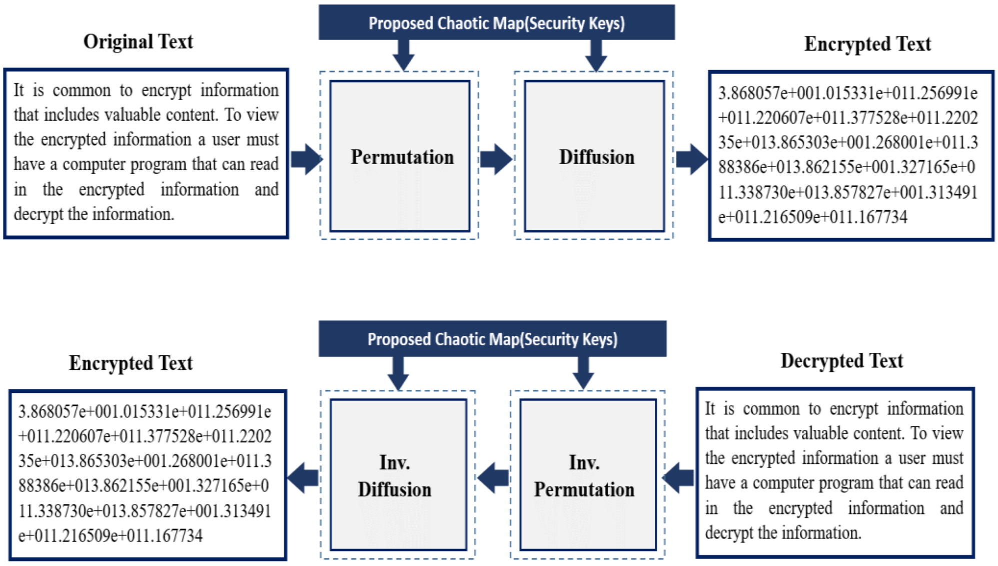
Encryption (and decryption) techniques based on chaotic maps are used to boost data security. This situation can be described by the chaotic map's nature, which is gravity, which is the chaotic map's output for each input; Property confusion, a tiny aberration of the local area, implies a huge aberration of space; the sensitivity of the starting value/control parameters, which is a minor change in the initial parameters/input parameters, includes large changes in the output value; The deterministic process involving incorrect alignment behavior is a simple approach that is extremely difficult to master.

Many deployments of chaotic maps on cryptographic systems, such as the described algorithm/scheme, are deployed for image and video encryption. Logistic maps and logistic map change are the most often utilized maps under chaotic conditions [62].

The chaotic map-based encryption (and decryption) systems are used to increase data safety. The chaotic character of the map, that is, the heaviness of any input, can explain this scenario. The distribution yields the same distribution for the map output; Because of sensitivity to the starting value / control parameter, a minor change in the input / initial value parameters results in a huge change in the output; The combination has the property that a small divergence in the local area implies a huge deviation in space [63].

The pseudorandom behavior of a deterministic process is referred to as deterministic dynamic; and a simple process, which implies a high level of complexity in the structure. Many deployments of messianic maps in encryption methods, including the introduced algorithm/scheme, are implemented for image and video encryption [63].

The structure of our text encryption/decryption is given in Figure (2.8).



It is common to encrypt information that includes valuable content. To view the encrypted information a user must have a computer program that can read in the encrypted information and decrypt the information.

3.868057e+001.015331e+011.256991e+011.220607e+011.377528e+011.220235e+013.865303e+001.268001e+011.388386e+013.862155e+001.327165e+011.338730e+013.857827e+001.313491e+011.216509e+011.167734

3.868057e+001.015331e+011.256991e+011.220607e+011.377528e+011.220235e+013.865303e+001.268001e+011.388386e+013.862155e+001.327165e+011.338730e+013.857827e+001.313491e+011.216509e+011.167734

It is common to encrypt information that includes valuable content. To view the encrypted information a user must have a computer program that can read in the encrypted information and decrypt the information.

Figure (2.8). Schematic illustration of the (a) encryption and (b) decryption processes of the text encryption scheme [61].

The Busy and Idle states sequentially explain the presence and absence of primary users, because occupied states mean operating intervals or PU presence, the secondary user can gain radio spectrum from the idle condition of the primary users.

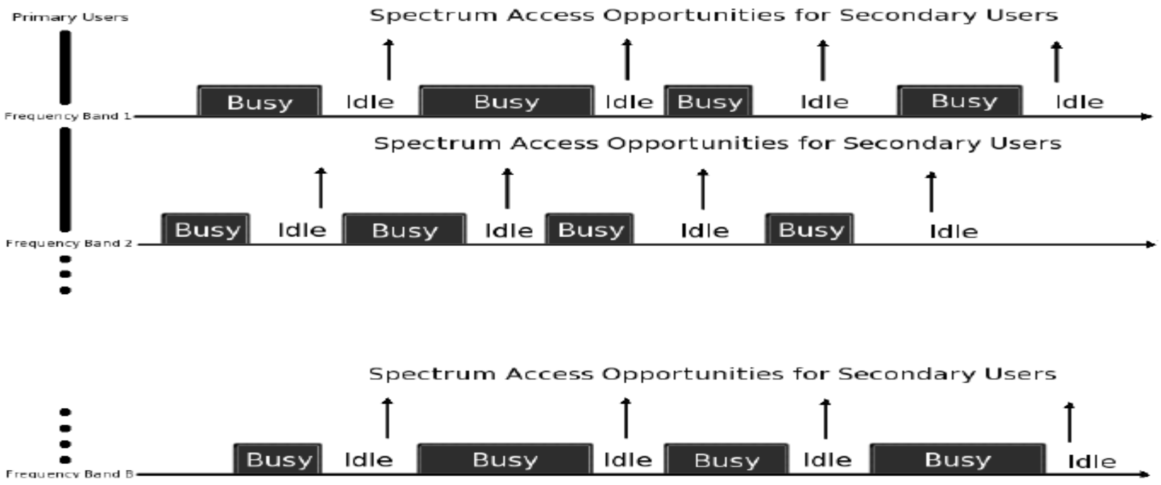


Figure (2.9) Busy and Idle state for primary user spectrum access [72]

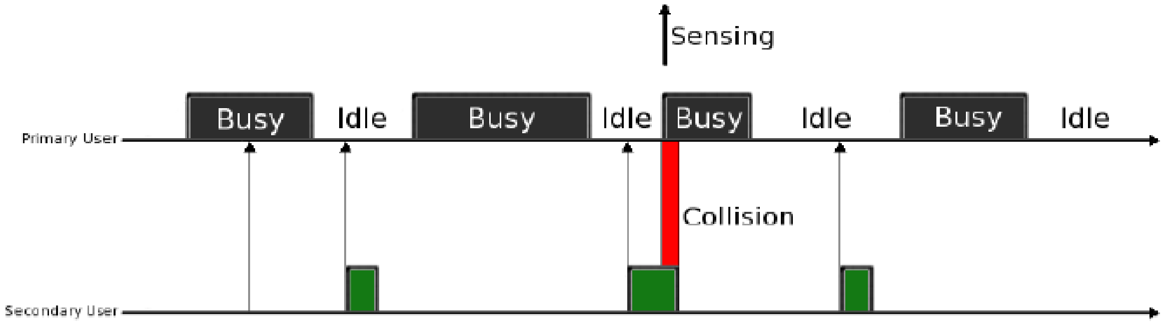


Figure (2.10) behavior of Primary and secondary users [72]

2.8 Keyword Recognition

Spectrum CR sensing to determine the proposed uninterrupted channel in the first section of the packet in order to send data messages and not detrimental The primary user called the Global Mobile Communication System (gsm) then decides which free or busy channel. When the simulator starts, data type values are entered as keyword parameters that provide the initial input to the cognitive network environment. Below explained this message:

2.8.1 Chaotic word Frame Format.

The top corner segmentation bits define the frame's key feature and the load segment (0-254 bytes) includes the primary data. The following components are provided and they are described in figure (2.11):

The proposed channel: the idle channel is a free channel that is used for broadcasting messages.

Frame ID: As a slot, it's a good fit in the frame ID, you can see which slot the frame will be conveying to There can only be one instance of a-frame identification per channel every communication cycle. A unique frame ID is assigned to each frame, which has a single slot. One to 2047 is the Frame ID range, while 0 is invalid. Invalid Frame ID 0

Data length: is used to define the size of a Fields of Encapsulation. Encapsulation size is set to 2 bytes (date length times 2 = encapsulation data size in bytes). This parameter encodes the size of the Encryption Field.

Source (Src): MAC source address describes.

Destination (Des): Destination (Des) Address of MAC

Control (Ctrl): description of the control information in the mac layer, such as RTS/CTS, to reduce collisions in messages.

Association: Specifies the safety mechanism utilized to obtain access to the chaotic CRWN.

Encapsulation: contain security elements for the system presented (plain text and CipherText) based on a "chaotic encryption method," developed using a c# programming language external library.

Data (keywords): Input keywords that are provided in an initial simulation state are specified to allow any word used on the cellular network to be entered.

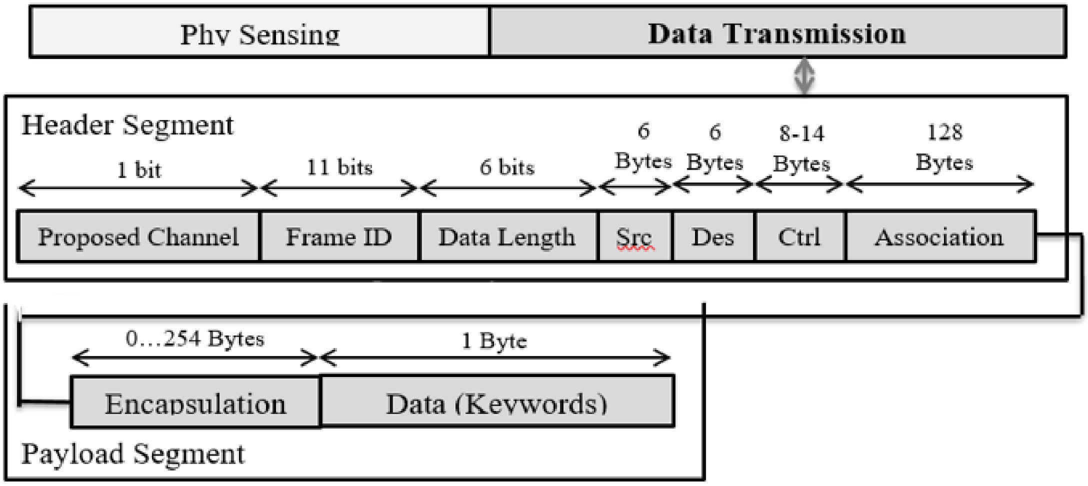


Figure (2.11) the chaotic word Frames Format [73]

The Control Frames

To improve a virtual carrier sense procedure, frames for RTS (Request to send) & CTS (Clear to sending). To avoid collisions, RTS/CTS is mimicked.

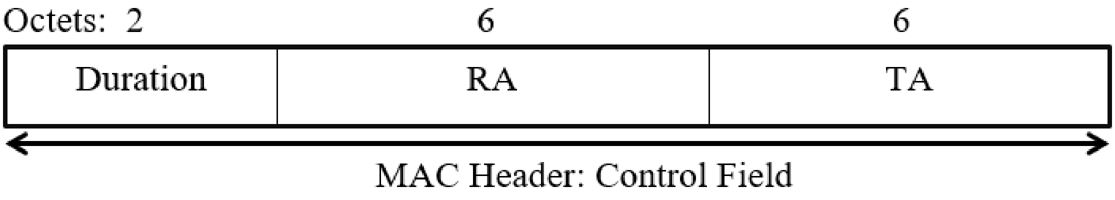
RTS (Request to Send) Frame

RTS framework format. It has a length of 14 bytes. Each octet is shown by (8 bits). Three fields are found in the RTS framework:

1. Duration: 2 bytes including the transmission time required for successive transmission frames.

2. RA (Receptor Address): 6 bytes of MAC Address of the station to which the frame is submitted;

3. TA (Transmitter Address): 6 bytes, Sender address showing the station MAC address of the message.



Octets: 2	6	6
Duration	RA	TA

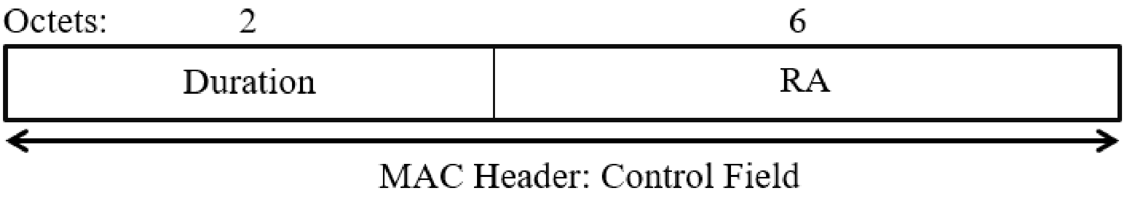
Figure (2.12) the RTS Frame Format [73] .

CTS (Clear to Send) & Acknowledgement(ACK) Frames

Formats of RTS and ACK frames. It is 8 bytes in length for each frame.

1- Duration: 2 octets = 16 bits.

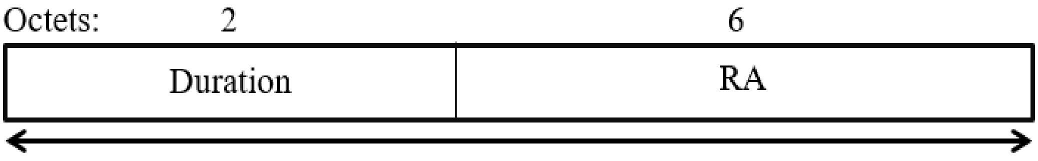
2- RA (Receiver Address): 6 octets = 48 bits.



Octets: 2	6
Duration	RA

Figure (2.13) the CTS Frame Format [74]

An acknowledgment frame sends to the transmitter to validating the data frame received by the receiver node. As duration always set to 0. It should be noted only in the (ACK) frame, in the field (Duration). To indicate the next frame request it is always set to zero.



Octets: 2	6
Duration	RA

Figure (2.14) the Acknowledgement Frame Format *[75]*

2.9 Simulation tools used to enhance the security of Cognitive Radio Network

In the following, typical simulation tools are explained: There are numerous types of tools and programming languages to mimic, however, the safety conception of the cognitive radio network.

1)MATLAB: is an advanced technical computing language. Computers, visuals, and programming environments are integrated. In addition, MATLAB features advanced data structures has integrated edit and debugging tools, and enables object-based programming. It also offers an up-to-date programming language environment. This makes MATLAB an outstanding teaching and research instrument. IN comparison to standard computer languages (e.g. C, FORTRAN), MATLAB offers several benefits for the resolution of technical difficulties. MATLAB is an interactive system with a fundamental data element that is not dimensioned. Since 1984 the software package has been available on the market and today is commonplace at most colleges and enterprises throughout the world [64].

2)NS2: It is an event-driven open-source simulator specially built for studies in the networks of computer communication. NS2 has been gaining enormous interest from business, academia, and government since it was founded in 1989. After years of continuous inquiry and improvement, NS2 currently includes modules for many of the network components, including routing, transportation layer protocol, and application. Researchers may simply utilize a simple programming language to set up a network and view findings provided by NS2 to analyze network performance. NS2 has, of course, become the most popular open-source network simulator and one of the most commonly used network simulators [65].

3)OMNeT++: It is accessible in open source and under the Academic General Licence, software for non-commercial use. OMNeT++ aimed to produce a sophisticated, open-source, discreet event simulation tool that may be applied by academic, educational, and research companies to model computer networks and distributed systems or parallel systems. OMNeT++ attempts to close the gap between open-source simulation tools such as NS-2 and costly business solutions such as OPNET. To run OMNeT++ on all popular systems, including Linux, Mac OS/X, and Windows, GCC Toolchain, or Microsoft VisualC++ Compiler are necessary. OMNeT++ stands for the framework approach. It provides the fundamental machines and tools for such simulations instead of supplying the components for the simulation explicitly in computer networks, queuing networks, or other domain systems [66].

4)OPNET: Model of a network simulation. Modeler is a network simulator that is widely used in academics and industry. Most network protocols, including wireless ones, are supported. The OPNET wireless base includes the Point Coordination Function (PCF) and Distributed Coordination Function (DCF). Modeling existing measuring equipment is also possible with OPNET Modeler [67].

Chapter Three

The Proposed System

3.1 Introduction

This chapter explains the mechanism that was followed in protecting the networks of the cognitive system, as it contains the most important steps that were followed and taken in order to provide a secure system from eavesdropping attacks, as it contains two methods: first way protected from passive eavesdropping attacks that are done allow secondary users who know them through their IP addresses to use the empty channels, but when any external user that they don't know and does not have an IP address it is considered an attack, they are not allowed to use the empty channel. The second way the chaotic encryption algorithm is used to protect messages from an active eavesdropping attack because the main advantage is that the chaotic signal appears to unauthorized users as noise, and the chaotic signals are very sensitive to the starting conditions.

A proposed safe keyword identification approach to increase the security of a cognitive radio network cellular network application with content awareness feature, for each message sent between CR nodes using an encryption chaos algorithm. The OMNET++ and the visual C# language are used to run all simulations.

3.2 Implementation and Interconnection algorithms of Secure Cellular Networks in CRN Architecture

"Cognitive Radio Network's" design is identical to other wireless networks based on the five transmission layers for transmitting and receiving data as well as diverse data types including text, sound, and video because the offered solutions are built on (Information) data form. Every concept will be represented by a c++ module influenced by OMNET++ simulations.

The functional side of each of these modules as C++ code will be investigated using the parameters we assumed during each section's growth. In each layer, the following algorithms explain the key material of the proposed scheme (Application Layer, Network layer, CR MAC Layer, Physical Layer, and so on). The suggested framework is built on C++, which is the foundation for developing libraries, and OMNET ++, which is based on it.

Figure (3.1) Each of these modules is depicted in the fixed architecture, as well as their linkage across layers as a control and data link, in order to provide adequate results depending on the statistics modules & simulation parameters, more details about the layers and how can use every layers in appendix B.

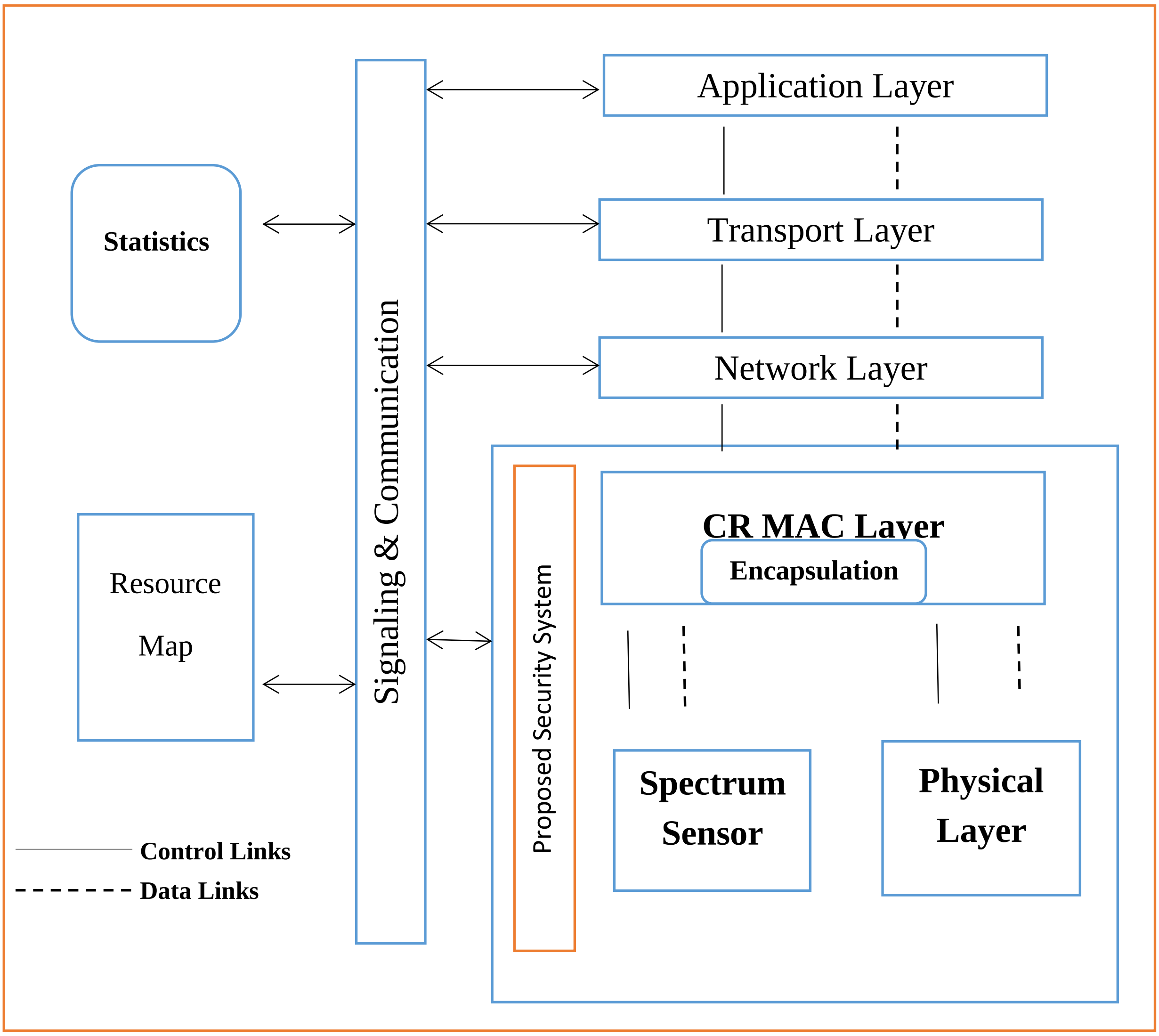


Figure (3.1) The architecture for cognitive radio [76]

PuNodes: this module was designed to generate PU activity patterns that matched the actual events found in the Global System for Mobile Communications (GSM). We've compiled a list of general measures for PU behaviors that mimic PU actions. All of these procedures are performed inside the (puGSM.cc and puGSM.h) directories.

puGSM: describing actions for each primary user using criteria and timers for presence and absence for the primary user, which influenced the secondary user's handoff and handover state without harming the primary user.

Table (3-1) Show the parameters of PUNodes and explain what meant everyone.

Parameters	**What the meant by**
PU Channel	Number of channel (1 - 10)
Busy Duration	Is a time interval during which the channel is continuously occupied without a break
Idle Duration	Is a period of time in which channel is ready and available
Power	Refers to the ability of a particular channel to control the decision making and behavior of the base station (PU) with the application layer provides a query when the PU comes or leaves the channel to check the power of each node; if the power is greater than the threshold, the node is purchased; otherwise, the node is free and can be used and measuring unit (Watt).
Threshold	It is the channel in which the movement of the channel is negligible or equal to the power value, which means that the channel is empty and the secondary user can use the channel and measuring unit (Watt).

Proposed Primary Users Behaviors: -

Primary user signals (input/output)

Phase 1: Create the case, which is represented by:

1- The recording of log files

2- Setting up the application layer timer with channels in its initial state (gsm1, gsm2, gsm3, gsm4, gsm5, gsm6, gsm7, gsm8, gsm9, gsm10)

3- Assumption of being idle, busy, power and threshold Each PU's a (gsm) duration is:

gsm1:

```
    PUChannel = 1;

    busyDuration = 0.0100;

    idleDuration = 0.0200;

    Power = 0.5;

    Threshold = 1;
```

gsm2:

```
    PUChannel = 2;

    busyDuration = 0.0200;

    idleDuration = 0.0300;

    Power = 0.6;

    Threshold = 1;

     Threshold = 1;
```

```
gsm3:
        PUChannel = 3;
        busyDuration = 0.0300;
        idleDuration = 0.0400;
        Power = 0.8;
gsm4:
         PUChannel = 4;
         busyDuration = 0.0500;
         idleDuration = 0.0400;
         Power = 5;
         Threshold = 1;
gsm5:
         PUChannel = 5;
         busyDuration = 0.0600;
         idleDuration = 0.0500;
         Power = 6;
         Threshold = 1;
gsm6:
         PUChannel = 6;
         busyDuration = 0.0700;
         idleDuration = 0.0600;
         Power=7;
         Threshold=1;
```

```
gsm7:
          PUChannel = 7;
          busyDuration = 0.0800;
          idleDuration = 0.0700;
          Power = 8;
          Threshold = 1;
 gsm8:
          PUChannel = 8;
          busyDuration = 0.0900;
          idleDuration = 0.0800;
          Power = 9;
          Threshold = 1;
gsm9:
           PUChannel = 9;
           busyDuration = 0.1000;
           idleDuration = 0.0900;
           Power = 10;
           Threshold = 1;
gsm10:
           PUChannel = 10;
           busyDuration = 0.1100;
           idleDuration = 0.1000;
```

Phase 2: Begin Functions of Handlers

1- Begin broadcasting through data rate to each connected device.

2- Indicating the status of transmission.

3- The broadcast has ended. With the precise recognized signal, PU END brings the PU communication to a close.

4- Indicating the end of the transmission

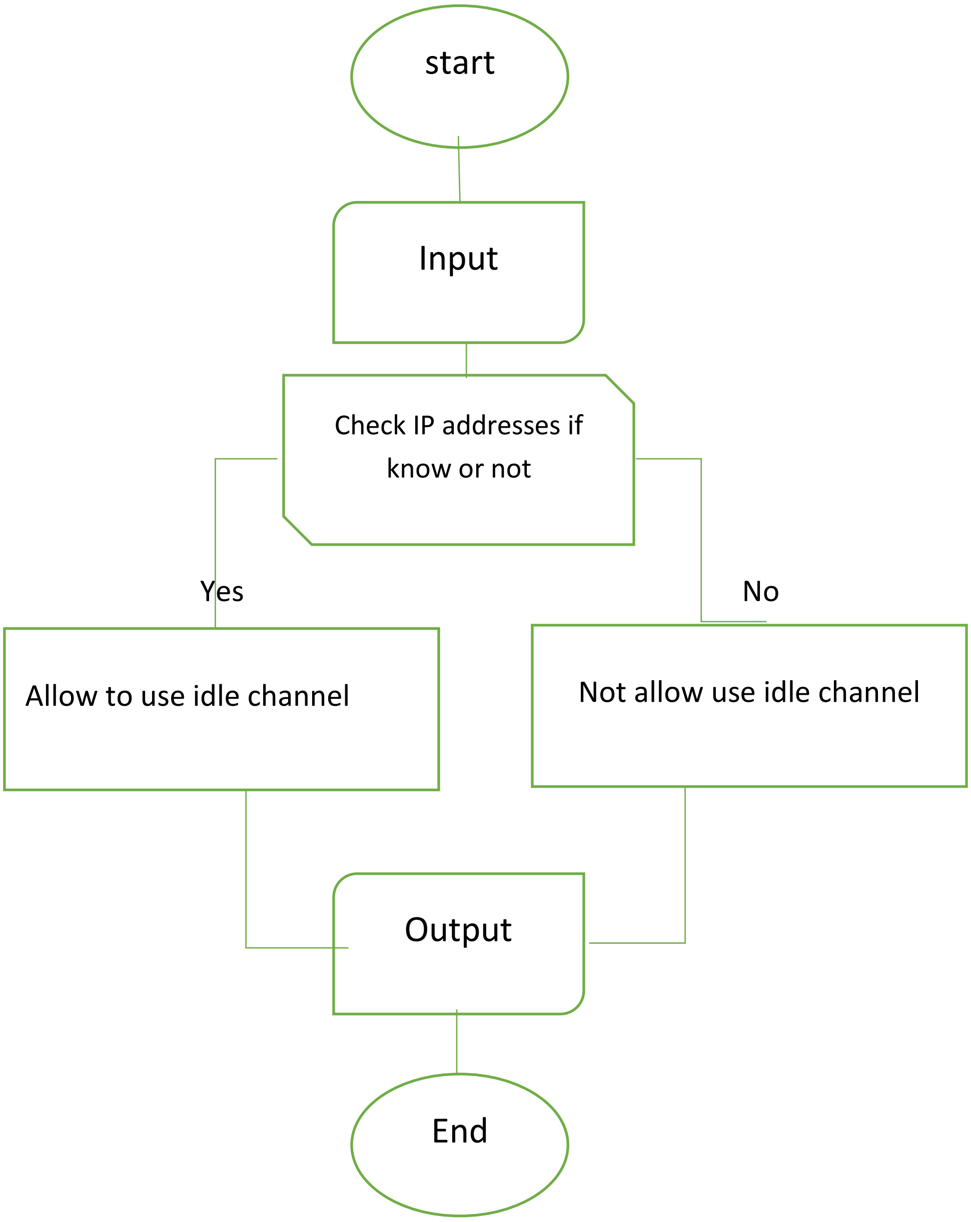
3.3 The Proposed Security System for Cognitive Radio Network

In order to provide protection for the cognitive radio network from the types of passive and active eavesdropping attacks, this was done in two main steps, as follows:

3.3.1 Protection from passive eavesdropping attack

Protection from passive eavesdropping attacks was done by defining secondary users who are allowed to use the spectrum by IP addresses so that users with prior knowledge of them are identified and allowed to use the spectrum and when an unknown user comes it is treated as an attack or an unauthorized user from Spectrum use

Proposed Protection from passive eavesdropping attacks


start
Input
Check IP addresses if know or not
Yes
No
Allow to use idle channel
Not allow use idle channel
Output
End

3.3.2 Protection from an active eavesdropping attack

The effect of an active eavesdropping attack is more than a positive eavesdropping attack, as it alters the content of the message and causes harm to the system. In order to protect messages, encrypted messages were used in the exchange process. In the first phase of runtime simulation we initiate c# programming language input Keywords Message exchanges between cellular networks and its equivalent encryption.CRN's Architecture Layers will be used to record these processes (DATA & CTRL Links). Following that, the outcomes and statistics of the proposed CRNs implementation in networks' cellular environments would be built.

OMNET++ was used to mimic all of the proposed system's processes within a 10-channel cognitive radio network. The general steps for the simulation process, as indicated in Figure (3.6), are as follows:

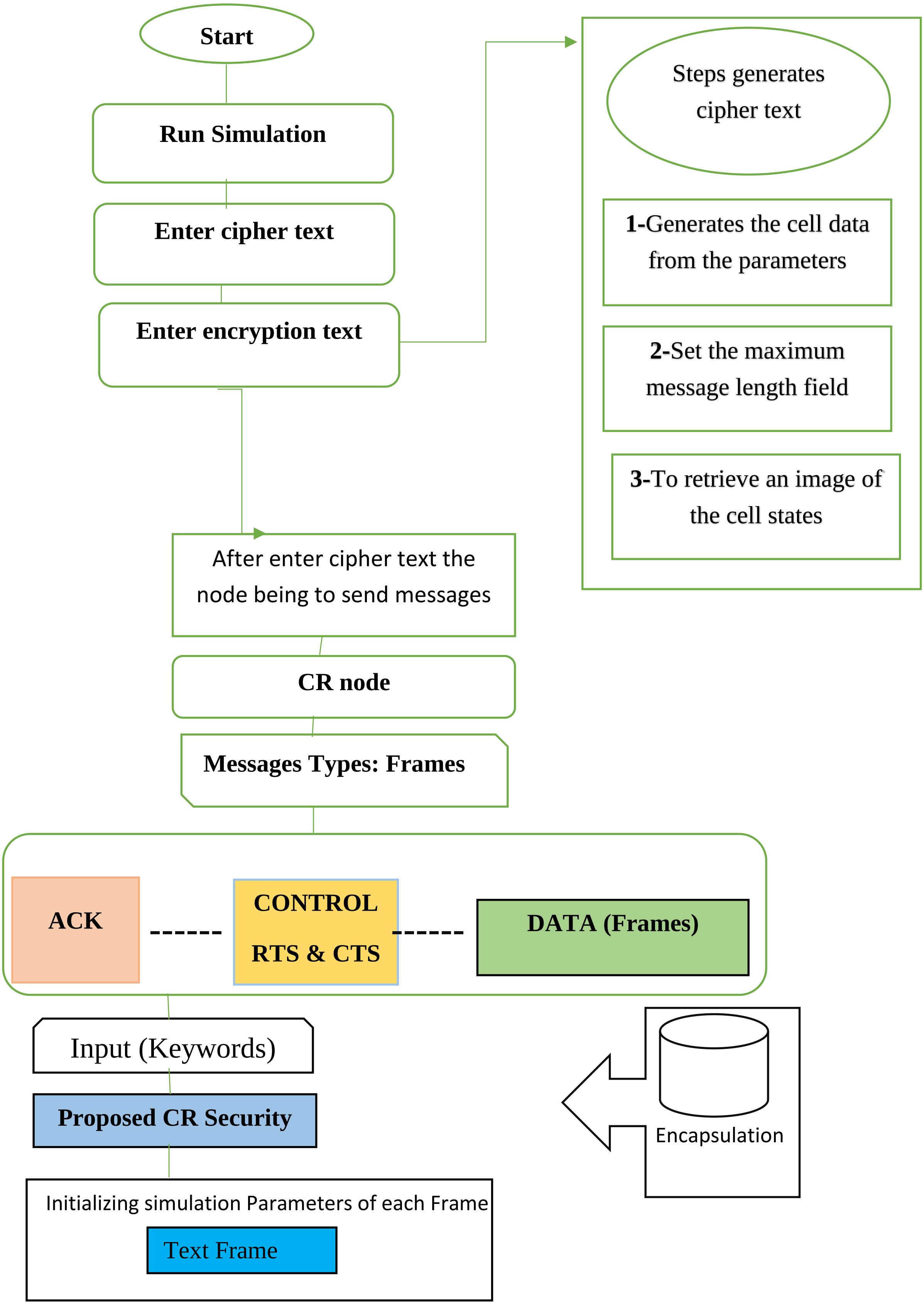

Start
Run Simulation
Enter cipher text
Enter encryption text
Steps generates cipher text
1-Generates the cell data from the parameters
2-Set the maximum message length field
3-To retrieve an image of the cell states
After enter cipher text the node being to send messages
CR node
Messages Types: Frames
ACK
CONTROL
RTS & CTS
DATA (Frames)
Input (Keywords)
Proposed CR Security
Initializing simulation Parameters of each Frame
Text Frame
Encapsulation

Figure (3.2) CRNs Security Scheme Block Diagram

Chaotic encryption algorithm

The generation of seemingly random number sequences as encryption keys is one of the difficulties in cryptography. A discrete computing model that is researched in automation theory can be used with a cellular automaton. Cellular automates and iterative arrays are sometimes known as cellular spaces. Mobile automatic devices may be directly utilized for creating visual or auditory multimedia content, for random cryptography or other reasons, and possibly for building parallel computers.

The design tools of the proposed textual content-encryption are primarily based on cellular automata chaotic map done explained in chapter three more detailed with non-linear transformation capabilities.

Key steps of the text encryption scheme.

_ **Input:** Plain-text file P_t.
_ **Output:** Cipher text file C_t.
_ **Begin**
1. **Convert** the plaintext file into a one-dimensional (1-D) array, S_{p_t}.
2. **Generate** the chaotic sequence by selecting two of the proposed maps (Equations (1)– (4): α = 0.9, $X_{(0)}$ = 0.1, and $Y_{(0)}$= 0.1).
3. **Change** the chaotic sequence into a uniformly distributed sequence by changing the initial values and parameters.
4. **Permute** Spt using the proposed chaotic map for the secret key
5. **Create** the new vector as: S_{p_t}= S_{k_t} (index).
6. **Adjust** and change Spt utilizing the proposed chaotic map and the accompanying condition:
S_{p_t} (i) = mod (round ($10^{12}S_{p_t}$ (i)), 256).
7. **Create** the diffused vector S_{D_t} = $S_{p_t} \oplus S_{k_t}$, where $\oplus$ denotes the bit-by-bit exclusive OR operation.
8. **Create** the final cipher text matrix C_t = reshape (S_{D_t}, P_t).
_ **End**

A cellular automatic simulation was the first step.

The system consists of two key components:

1) Using the CAGrid class, you can run a simulation of mobile automation quickly. It provides a list of Cell objects, grid constructing methods, and attaching each cell to its neighbors, rules execution methods and generations growing, and data retrieval ways as a byte or Boolean arrays.

2)In order to provide cryptographic functionalities, the encryption class uses CAGrid.

Static methods for creating huge blocks of key data are provided for the CAEncryption class. The data are extracted from a grid by means of a progressive manner and re-executed to provide you more data. For symmetrically encrypting streams and files.

An encoded file is stored in a class that can be replicated to the disk. The original filename is contained as a property for facilitating data decryption. A byte array is used to store the encrypted file. The Random class initializes the grid with a seed value by using all static encryption methods. Installing the approaches for producing encryption key data from a bitmap are used the CAEncryption class. The basic system form is FrmCellularEncryption. All are connected together.

Proposed the system A cellular automatic simulation

1- **created a basic cell grid**

```
protected int get Index (int x, int y)
{
return (x *_height) + y;
 }
```

2- **execute a CA grid generation utilizing the Fredkin Rule**

(Which is based on the odd or even number of live neighboring cells)

```
public void RunFredkinRule ()
{
// enumerate the cells: foreach (var cell in _cells)
 {
 if (cell.LivingNeighbours % 2 == 0)
cell.NextState = false;
else
cell.NextState = true;


} Commit ();
```

3- **run Conway rules (original set of four rules)**

```
public void RunConwaysRule ()
{
// proces conways rules for game of life for each cell
// enumerate the cells:
 foreach (var cell in _cells)
{
// count the cells neighbours:
int neighbours = cell.LivingNeighbours;
 // a living cell with less than 2 living neighbours will die of loneliness
 if (cell.State && neighbours < 2) cell.NextState = false;
 // a living cell with 2 or 3 neighbours remains alive
if (cell.State && (neighbours == 2 || neighbours == 3))
cell.NextState = true;
// a living cell with more than 3 neighbours dies of overcrowding.
if (cell.State && neighbours > 3) cell.NextState = false;
// an empty cell with exactly 3 neighbours becomes alive.
if (! cell.State && neighbours == 3) cell.NextState = true; }
// commit the changes
Commit ();
```

4- public void BuildFromPseudoRandomNumbers (int seed, int width, int height)

```
{
BuildGrid (width, height);
Random rnd = new Random(seed);
foreach (var cell in _cells)
{
if (rnd.NextDouble() > 0.5)
cell.State =  true;
}
```

5- public bool [] GetBinaryCellData (int len)

```
bool [] data = new bool[len];
for (int i = 0; i < data.Length; i++)
{
data[i] = _cells[i]. State;
}
return data;
```

6- public bvte [] GetBvtes (int bytes)

```
{
// initialize a bit-array:
BitArray ba = new BitArray (GetBinaryCellData (bytes * 8));
 // initialize the output array:
 byte [] buffer = new byte[bytes];
// copy & return:
ba.CopyTo(buffer, 0);
 return buffer;
```

3.4 Generating Large Blocks of Key Data:

The quantity of data from a grid is based on the grid's size. The larger the grid, the longer it needs to be processed.

Furthermore, the.NET list object index field only measures 24 bits. The content is therefore limited to 16,7 million. The maximum data created by a single block is only 1 bit per item and is 2 MB, which is somewhat restrictive.

It is possible to read a fresh data block from a grid by reading the contents of the grid and then re-executing the CA rules. It is possible to construct an unlimited data set by starting with a small block that yields 1KB of data and continuously repeating the CA rules.

Generating Large Blocks of Key Data

1-return a linear array of Booleans representing the cell states.

```
 bool [] data = new bool[len];
 for (int i = 0; i < data.Length; i++)
 {data[i] = _cells[i]. State;}
 return data;
```

2- return a byte-array of all the available cell data.

```
 // initialize a bit-array:
 BitArray ba = new BitArray(GetBinaryCellData ());
 // calculate the number of whole bytes:
 int byteLen = ba.Length / 8;
 if (ba.Length % 8 != 0)
     byteLen++;
// To hold the bytes, make a buffer:
 byte [] buffer = new byte[byteLen];
 // fill the buffer from the byte-array:
 ba.CopyTo(buffer, 0);
 // return the bytes:
 return buffer;
```

3-return a byte array of the specified number of bytes from the cell data.

```
// calculate the required number of bits.
```

```
int bitLen = bytes * 8;
if (bitLen > _cells.Count)
    throw new ArgumentException ("Insufficient Cells");
// to create a bit-array:
BitArray ba = new BitArray (GetBinaryCellData (bytes * 8));
// set up the output array:
byte [] buffer = new byte[bytes];
// copy from the bit-array into the byte array.
ba.CopyTo(buffer, 0);
return buffer;
```

3.5 Encode a string using the binary key-data. the key data must be longer than the message.

1- check the length of the key-data:

```
if (message.Length > keyData.Length)
   throw new ArgumentException ("Insufficient Key Data");
```

2- use ASCII encoding to get an array of bytes from the message string:

```
byte [] msgBytes = Encoding.ASCII.GetBytes(message);

byte [] trimData = new byte [msgBytes.Length];
```

3- both bit-arrays must be the same length, copy out the required number of bytes from the key-data array:

```
Array.Copy(keyData, trimData, trimData.Length);
```

4- create bit-arrays from the message data & key-data

```
BitArray msg = new BitArray(msgBytes);

BitArray key = new BitArray(trimData);
```

5- XOR the two arrays:

```
BitArray output = msg.Xor(key);
```

6-copy the output back over the message array:

```
output.CopyTo(msgBytes, 0);
```

7- use base-64 to return the binary data as a printable string:

```
    return Convert.ToBase64String(msgBytes);
}
```

3.6 Decode the encoded string.

1-restore the original bytes from the base-64 string:

```
        byte [] msgBytes = Convert.FromBase64String(message);

        byte [] trimData = new byte [msgBytes.Length];
```

2-copy the required number of bytes from the key data

```
        Array.Copy(keyData, trimData, trimData.Length);
```

3- xor the binary data to restore the original bits

```
        BitArray msg = new BitArray(msgBytes);

        BitArray key = new BitArray(trimData);

        BitArray output = msg.Xor(key);
```

4-copy the translated bits back into the message array

```
        output. CopyTo (msgBytes, 0);
```

5-recreate the original string using ASCII encoding.

```
        return Encoding.ASCII. GetString(msgBytes);

    }
```

Chapter Four

Simulation, Results, and Discussion

4.1 Introduction

This chapter simulates and discusses the effects of an eavesdropping attack in a cognitive radio network, as well as the recommended security system described in chapter three. The suggested system has been simulated using OMNET++ and the C# programming language to implement encryption and decryption keywords. We chose OMNET ++ because it is simple to use with the Windows operating systems (Tkenv) graphical user interface (GUI). This GUI has several tracing, debugging, and execution features:

1) It is recommended throughout the main development simulation stage since it allows for a detailed view of the simulation state at any point during the execution timeline.

2) Keep an eye on what's going on inside the network.

3) The learning flexibility, which is dependent on the C++ programming language.

4) Contains several (Frameworks, Libraries, Models, and so on) that save time and effort for researchers when conducting research simulations in real-world settings.

5) In the Windows operating system, there are no restrictions for the installation condition. All communication in the Cognitive Radio Network takes place on a primary-secondary user paradigm, with primary users acting as base stations and secondary users acting as networks cellular, according to the basic network architecture.

The concept of eavesdropping is reinforced in cognitive radio networks where there are two types of eavesdropping, passive eavesdropping that affects primary users and only monitors communication without any change. And an active eavesdropping attack, this type of attack changes the content of the sent message and affects the communication process.

During the course of this thesis, the chaotic algorithm is used to improve the security of the cognitive radio network. In addition, the Frequency-hopping spread spectrum system represents a spread spectrum approach (FHSS). The network encryption systems' keywords were implemented using the outside library in C # to get the encrypted text and then insert it into the implementation interface to be exchanged among network nodes.

The proposed system was divided into five parts. The first part of the cognitive radio network has ten primary users and four secondary users, and a normal transmission without any effect. The second part of the cognitive radio network contains ten primary users and four secondary users, as well as a passive eavesdropping attack, which affects the primary users and monitors the connection only without any change. In the Part three, the primary user is protected from passive eavesdropping attacks by allowing only secondary users that they know to use empty channels, but when any external user they don't know comes in, it is considered an attack, and they are not allowed to use the empty channel. The fourth part of the cognitive radio network contains ten primary users and four secondary users, in addition to an active eavesdropping attack, this type of attack changes the content of the sent message and affects the communication process. In the fifth part, it was clarified how to send encrypted messages, as the chaotic algorithm was used to start the encryption externally, which means that all steps are done in a second program, where the output after the completion of the encryption process is the entry of messages into cognitive radio network.

The simulation parameters for all case studies (the whole proposed system in the OMNET++ simulator) are listed in the table below (4-1).

Parameters	**Value**
Simulation Time	5 m
Total Number of Frames	1024
Sensing interval	0.05 MS
Proposed Channel	1 or 2 or 3
Arrival Rate of PU	Variable 0.5-1s
Duration of PU TX	0.5s
The total number of nodes	4 SU , 10 PU
Layer of MAC	802.11b standard
Type of MAC	String Message

4.2 Case study normal of the Cognitive Radio Network

This network was created within the OMNET++ emulator without a security mechanism to imitate the network requirements of the cognitive node. This network configuration has 10 primary users and 4 secondary users.

Each cognitive radio node consists of five communication layers: the application layer, the transport layer, the network layer, the MAC layer, and the physical layer. Different signals are sent through different layers, and statistics are compiled based on simulation parameters. The base station (PU) with the application layer provides a query when the PU comes or leaves the channel to check the power of each node; if the power is greater than the threshold, the node is purchased; otherwise, the node is free and can be used.

The result of implementing this topology within simulation time of about (5 minutes) given (7) active nodes through the entire network as well as (3) idle nodes.

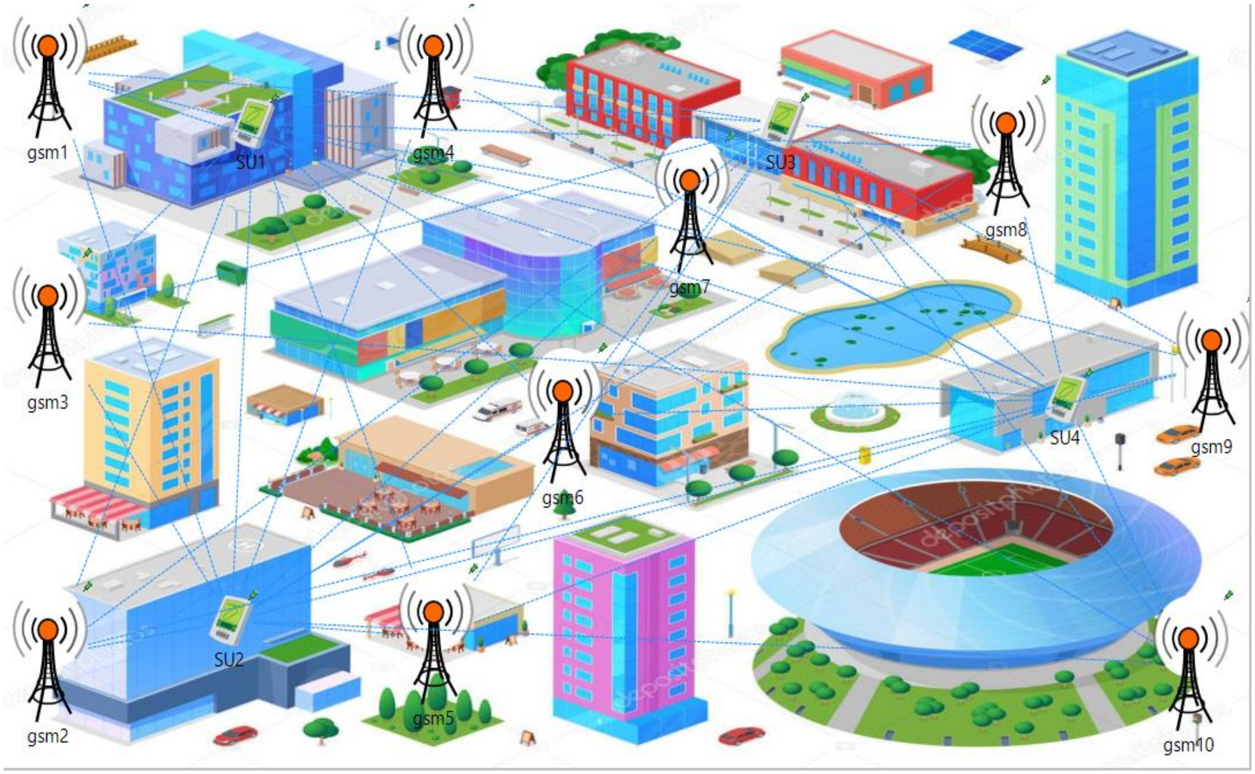


Figure (4.1) *Topology of CRNs.*

The signal values for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-2). (SU1). The transmission result for the (Req1) unit is shown in Figure (4-2).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**1**	sensingSignal	**1.1**

Table (4-2) application layer request, mac layer and spectrum sensing values.

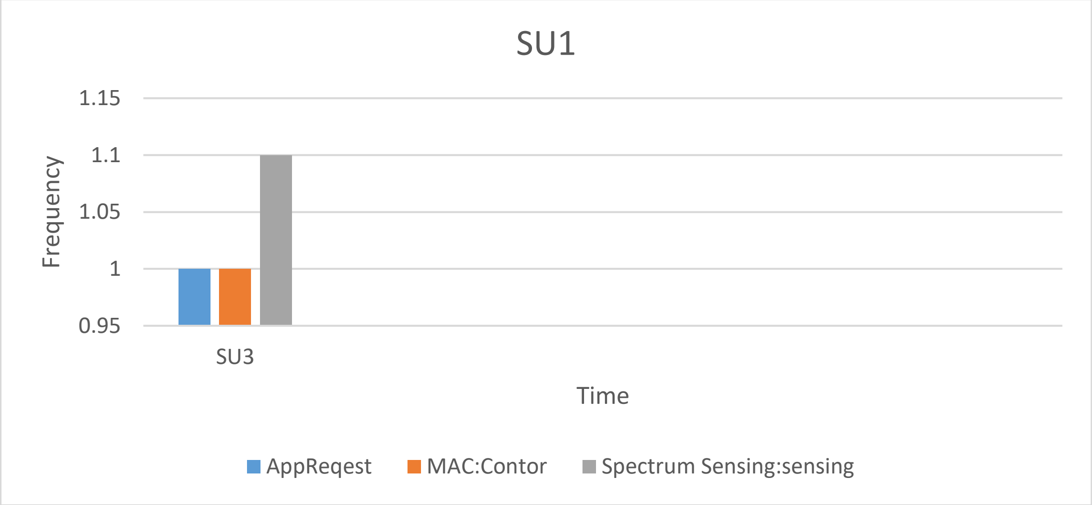


Figure (4.2) Statistical results from Transmitter SU1 unit

The results for the data and sensing signals in the receiver Req1 unit are summarized in Table (4-3). The receiver unit's results are shown in Figure (4.3).

MAC Layer		**Spectrum Sensing**	
dataSignal	**44**	sensingSignal	**6.7**

Table (4-3) Values from receiver Req1 unit.

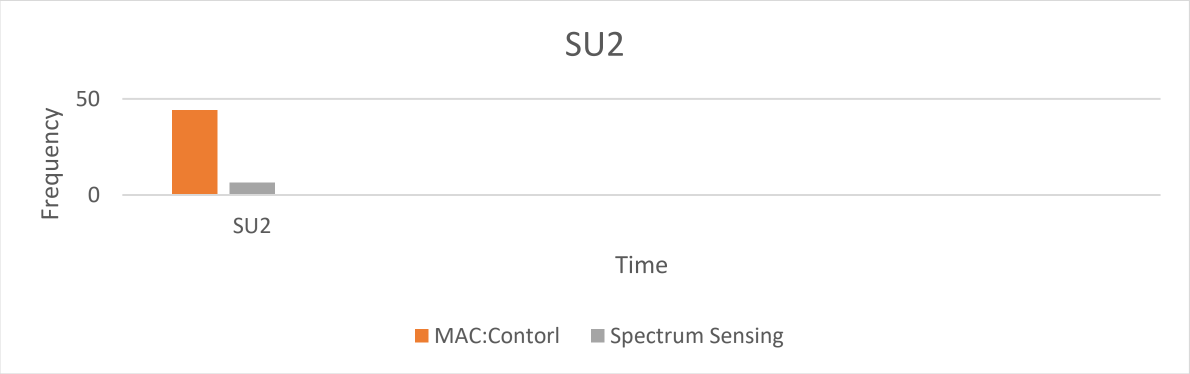


Figure (4.3) Statistical results from Receiver Req1 unit

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-4). (SU3). The transmission result for the (Req2) unit is shown in Figure (4.4).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**1**	sensingSignal	**5.8**

Table (4-4) Application layer request, mac layer and spectrum sensing values.

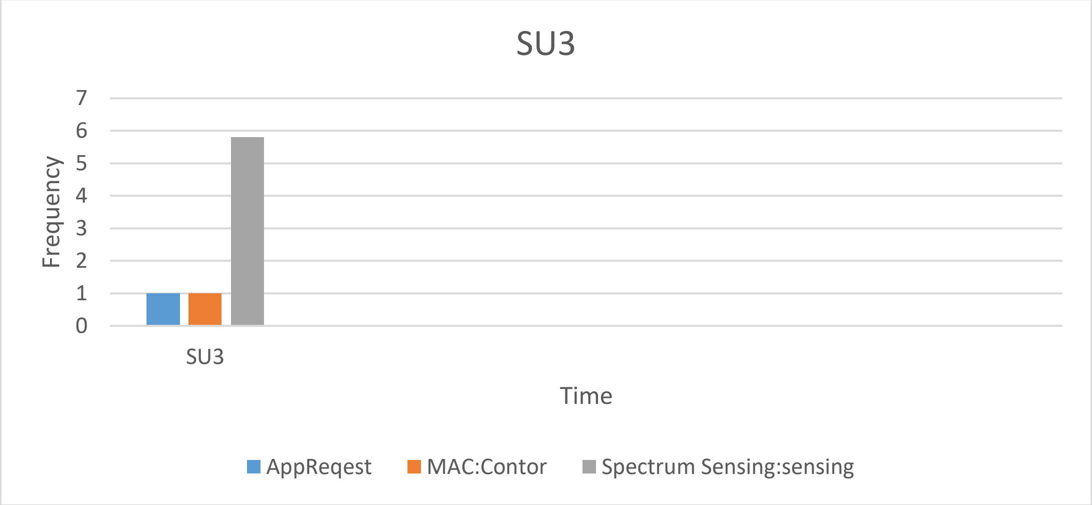


Figure (4.4) Statistical results from Transmitter SU3 unit

Table (4-5) summarizes the results for data signals and sensing signals in the receiver Req2 unit. while Figure (4.5) shows the results statics for the receiver unit.

MAC Layer		**Spectrum Sensing**	
dataSignal	**43**	sensingSignal	**6.4**

Table (4-5) Values from receiver Req2 unit

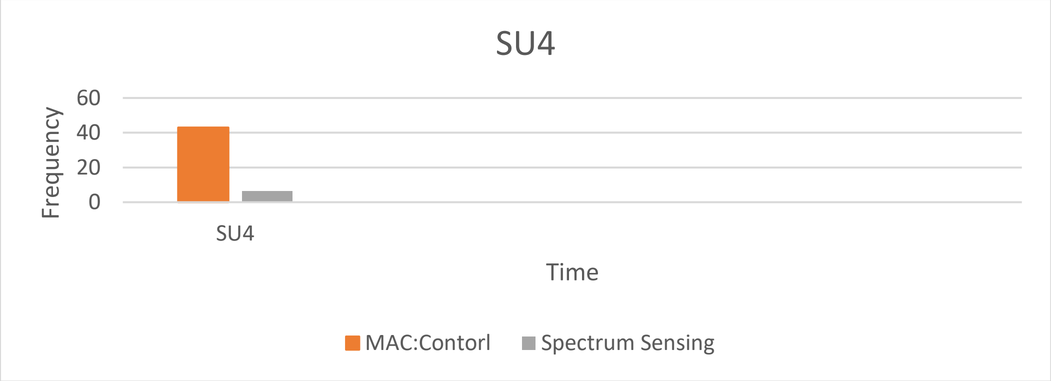


Figure (4.5) Statistical results from Receiver Req2 unit

Figure (4.6) depicts the difference in data message counts between (SU2 and SU4) receivers. Table (4-6) also demonstrates how to count data signals using receivers.

Receiver	Data Signal (Frames)
SU2	44
SU4	43

Table (4-6) Data Signal for all receivers.

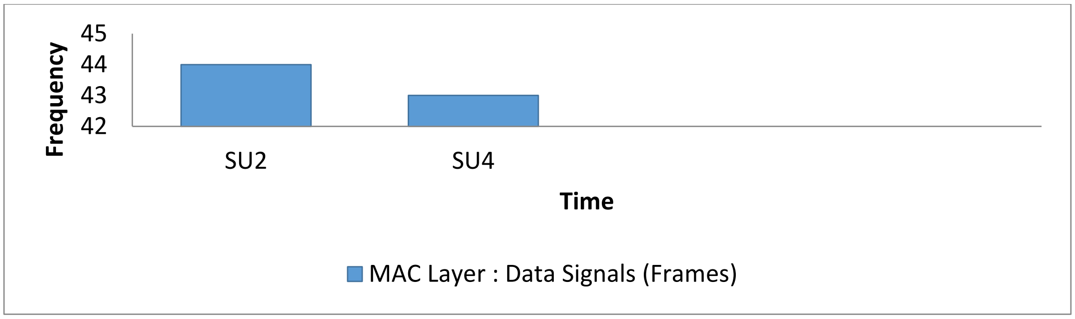


Figure (4.6) Statistical results from all active receiver units.

4.3 Case Study of passive eavesdropping attack

We simulate a passive eavesdropping attack on the primary user in this case study, which only impacts the primary users and observes the connection without making any changes. This network topology is presented in the same way as the proposed system topology, with ten primary users and four subsidiary users, as well as a passive eavesdropping assault.

The simulation length for this case study is roughly 5 minutes, similar to the first case study (with the suggested system), therefore we receive (7) active nodes and (3) idle nodes for the entire simulation time. The network topology is depicted in Figure (4.7).

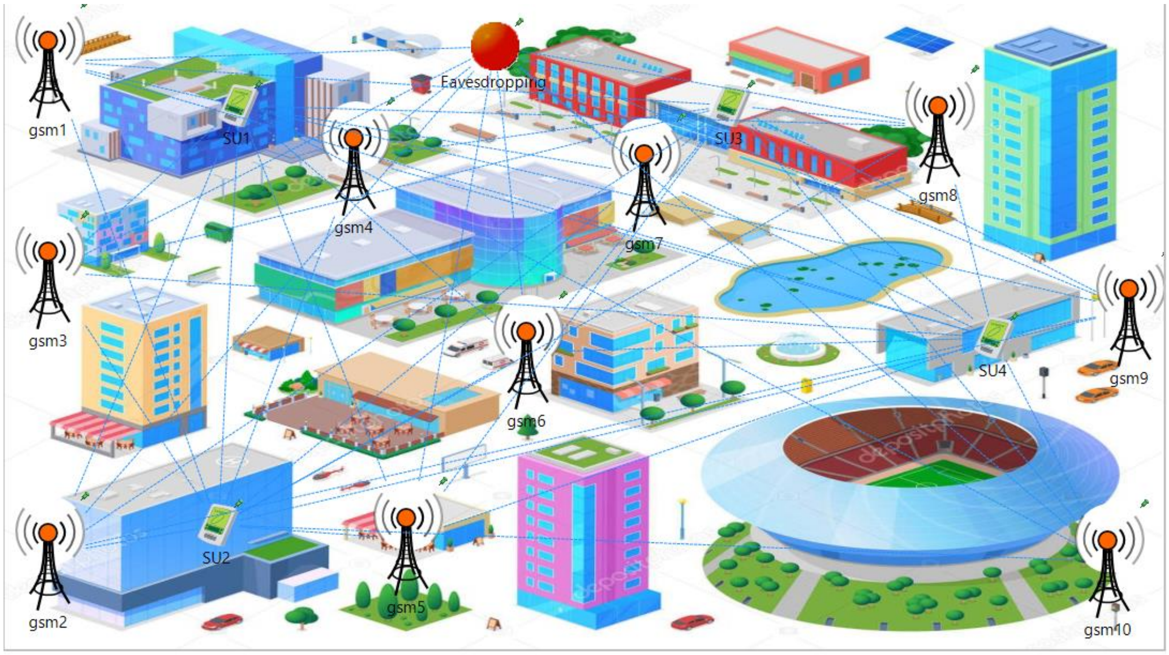


Figure (4.7) CRNs topology in networks cellular with passive eavesdropping attack.

The signals for the application layer, mac layer, and spectrum sensing that are collected interconnection layers (PHY-mac layer) in the transmitter unit are summarized in Table (4-7). The transmission result for the SU1 unit is shown in Figure (4.8).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**0.8**	sensingSignal	**6.2**

Table (4-7) *Application layer request, mac layer and spectrum sensing values.*

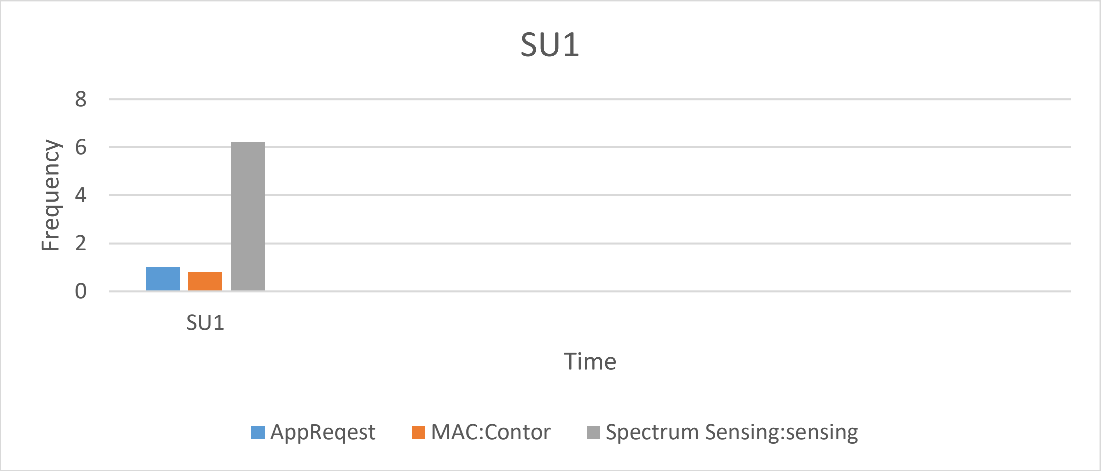


Figure (4.8) *statistical results from transmitter SU1 unit*

The results for the data and sensing signals in the receiver Req1 unit are summarized in Table (4-8). The receiver unit's results are shown in Figure (4.9).

MAC Layer		**Spectrum Sensing**	
dataSignal	**48**	sensingSignal	**6.8**

Table (4-8) Values from receiver Req1 unit.

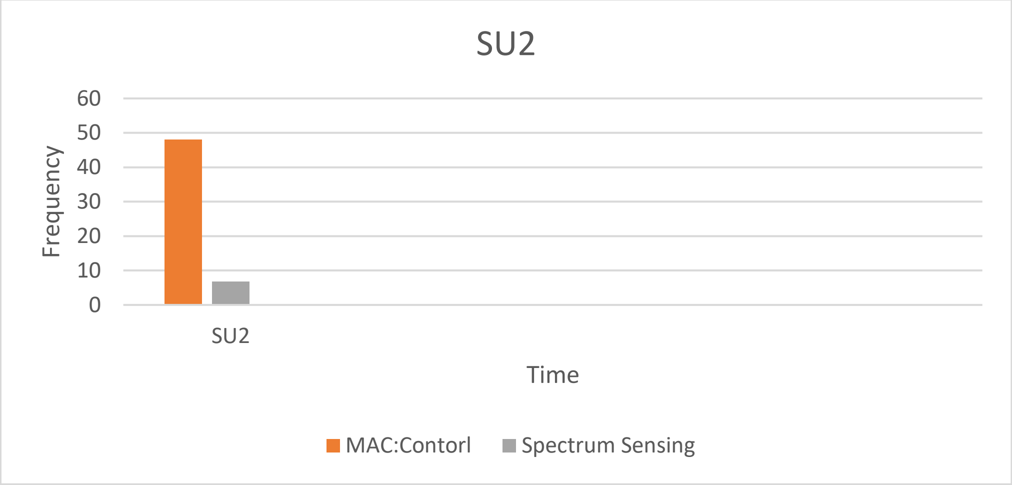


Figure (4.9) *Statistical results from Receiver Req1 unit*

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-9). (SU3). The transmission result for the (Req2) unit is shown in Figure (4.10).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**1**	sensingSignal	**6.1**

Table (4-9) Application layer request, mac layer and spectrum sensing values.

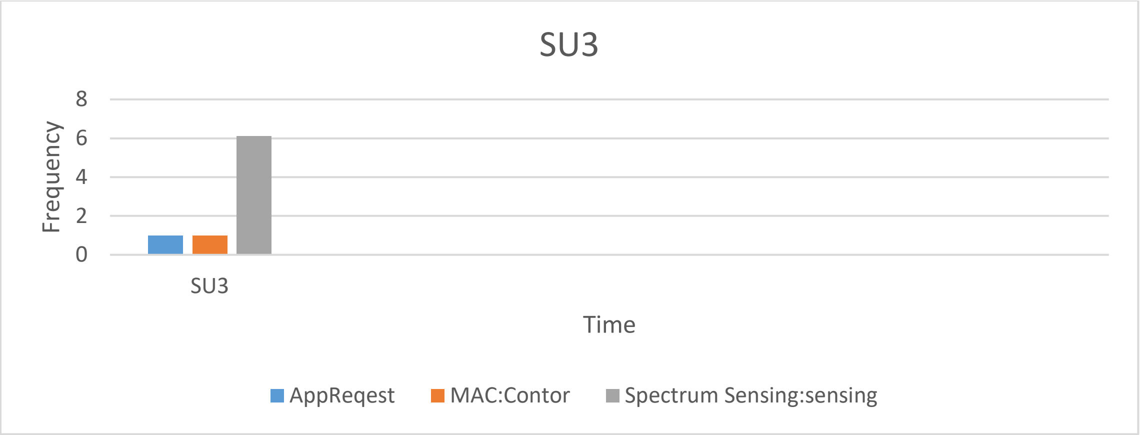


Figure (4.10) Statistical results from Transmitter SU3 unit

Table (4-10) summarizes the results for data signals and sensing signals in the receiver Req2 unit. while Figure (4.11) shows the results statics for the receiver unit.

MAC Layer		**Spectrum Sensing**	
dataSignal	**47**	sensingSignal	**7.1**

Table (4-10) Values from receiver Req2 unit.

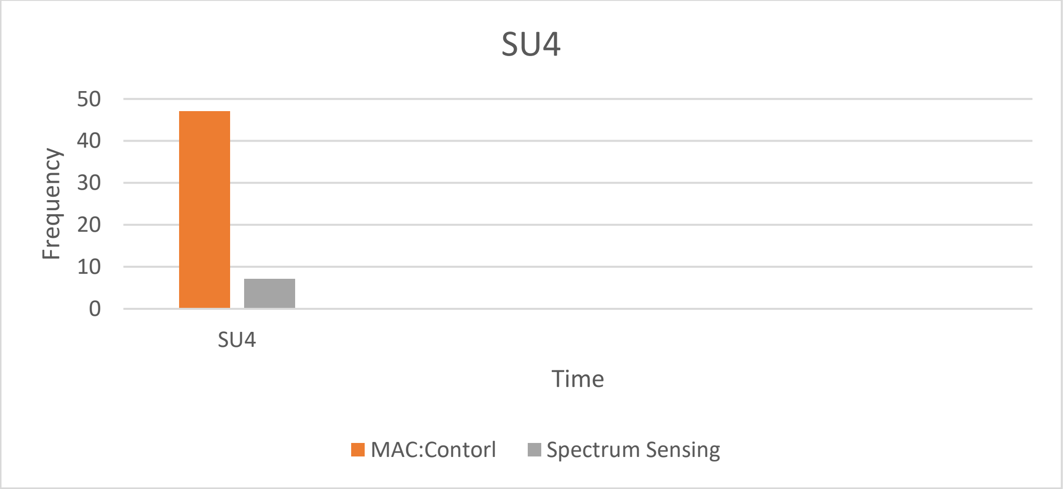


Figure (4.11) Statistical results from Receiver Req3 unit

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4.11). (Passive Eavesdropping). The transmission result for the (Passive Eavesdropping) unit is shown in Figure (4.12).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**1**	sensingSignal	**6.1**

Table (4-11) Application layer request, mac layer and spectrum sensing values

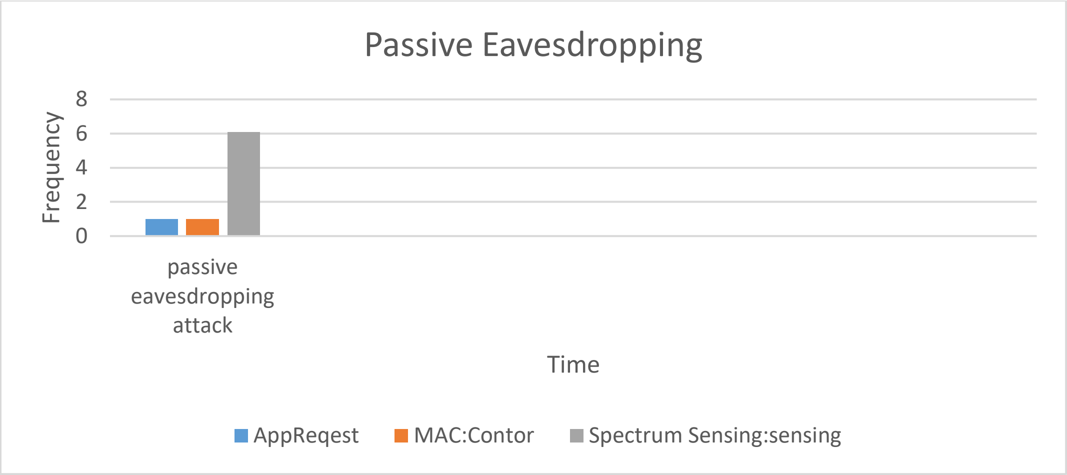


Figure (4.12) Statistical results from Transmitter Passive Eavesdropping unit

Figure (4.13) depicts the difference in data message counts between (SU2 and SU4) receivers. Table (4-12) also demonstrates how to count data signals using receivers.

Receiver	Data Signal (Frames)
SU2	48
SU4	47

Table (4.12) Data Signal for all receivers.

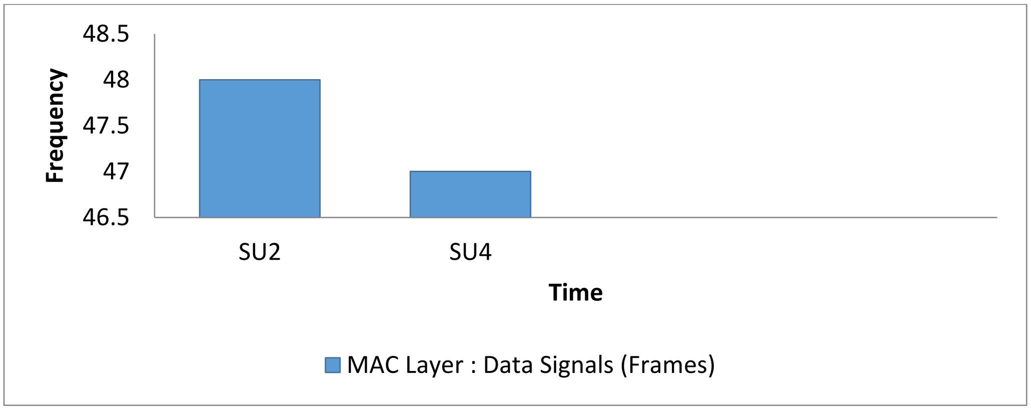


Figure (4.13) Statistical results from all active receiver units.

4.4 Case Study of protection from passive eavesdropping attack

The primary user is protected from passive eavesdropping attack by allowing only secondary users that they know to use empty channels, but when any external user they don't know comes in, it is considered an attack, and they are not allowed to use the empty channel. This network topology is presented in the same way as the proposed system topology, with ten primary users and four subsidiary users, as well as a passive eavesdropping assault.

The simulation length for this case study is roughly 5 minutes, similar to the first case study (with the suggested system), therefore we receive (7) active nodes and (3) idle nodes for the entire simulation time.

The signals for the application layer, mac layer, and spectrum sensing that are collected interconnection layers (PHY-mac layer) in the transmitter unit are summarized in Table (4-13). The transmission result for the SU1 unit is shown in Figure (4.14).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**0.8**	sensingSignal	**15**

Table (4-13) Application layer request, mac layer and spectrum sensing values.

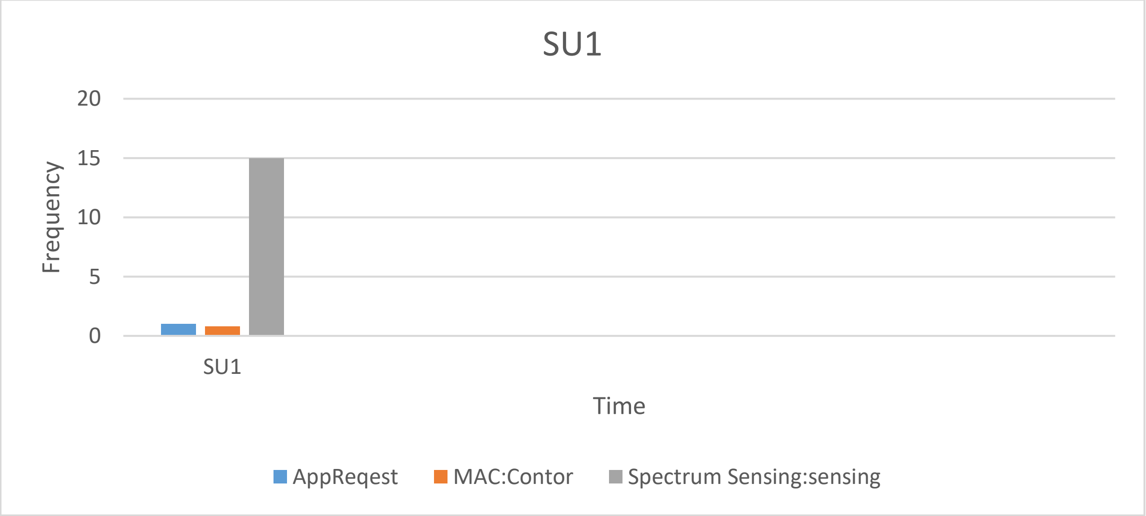


Figure (4.14) statistical results from transmitter SU1 unit

The results for the data and sensing signals in the receiver Req1 unit are summarized in Table (4-14). The receiver unit's results are shown in Figure (4.15).

MAC Layer		**Spectrum Sensing**	
dataSignal	**518**	SensingSignal	**13**

Table (4-14) Values from receiver Req1 unit.

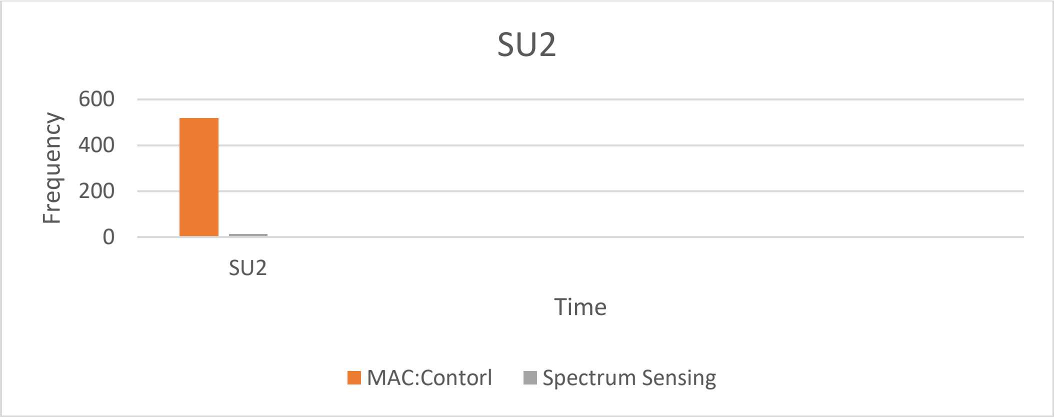


Figure (4.15) Statistical results from Receiver Req1 unit

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-15). (SU3). The transmission result for the (Req2) unit is shown in Figure (4.16).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**1**	sensingSignal	**27**

Table (4-15) Application layer request, mac layer and spectrum sensing values.

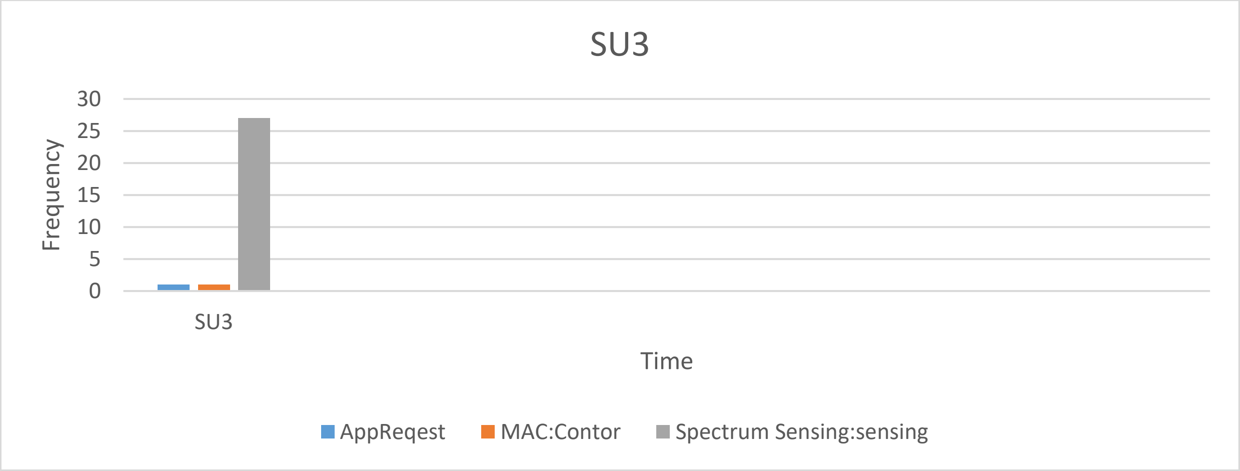


Figure (4.16) Statistical results from Transmitter SU3 unit

Table (4-16) summarizes the results for data signals and sensing signals in the receiver Req2 unit. while Figure (4.17) shows the results statics for the receiver unit.

MAC Layer		**Spectrum Sensing**	
dataSignal	**506**	sensingSignal	**21**

Table (4-16) Values from receiver Req2 unit.

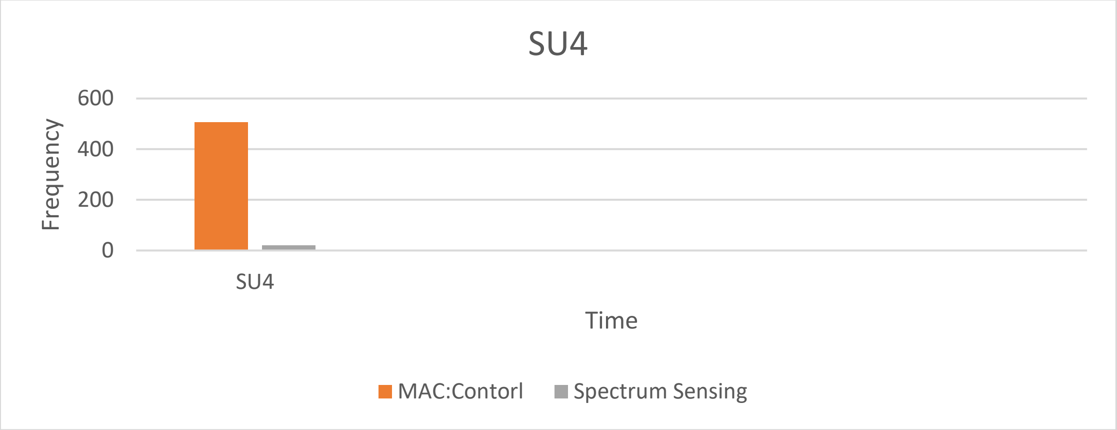


Figure (4.17) Statistical results from Receiver Req2 unit

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-17). (Passive Eavesdropping). The transmission result for the (Passive Eavesdropping) unit is shown in Figure (4.18).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**0**	sensingSignal	**15**

Table (4-17) Application layer request, mac layer and spectrum sensing values.

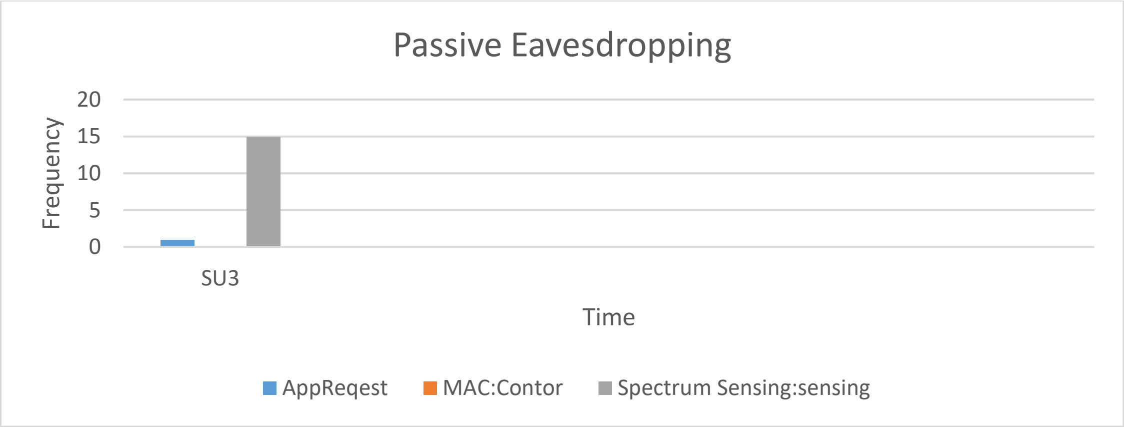


*Figure (4.*18) *Statistical results from Transmitter Passive Eavesdropping unit*

Figure (4.19) depicts the difference in data message counts between (SU2 and SU4) receivers. Table (4-18) also demonstrates how to count data signals using receivers.

Receiver	**Data Signal (Frames)**
SU2	518
SU4	506

Table (4-18) Data Signal for all receivers.

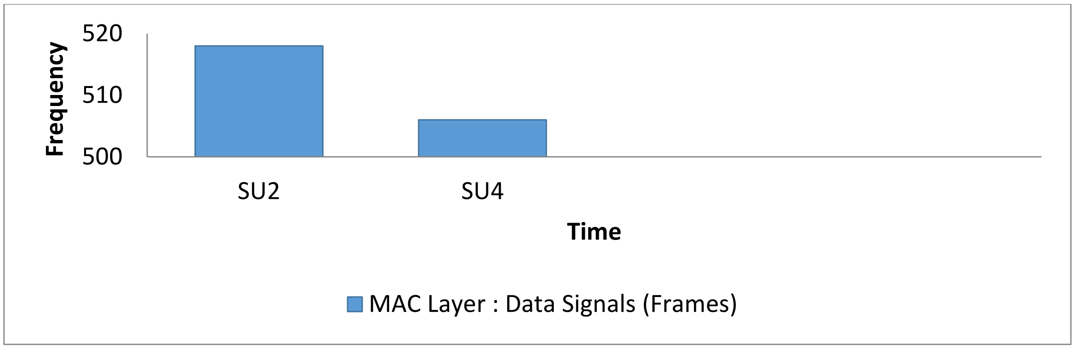


Figure (4.19) Statistical results from all active receiver units.

4.5 Case Study of an active eavesdropping attack

We simulate an active eavesdropping attack this type of attack changes the content of the sent message and affects the communication process. This network topology is presented in the same way as the proposed system topology, with contains ten primary users and four secondary users, in addition to an active eavesdropping attack.

The simulation length for this case study is roughly 5 minutes, similar to the first case study (with the suggested system), therefore we receive (7) active nodes and (3) idle nodes for the entire simulation time. The network topology is depicted in Figure (4.20).

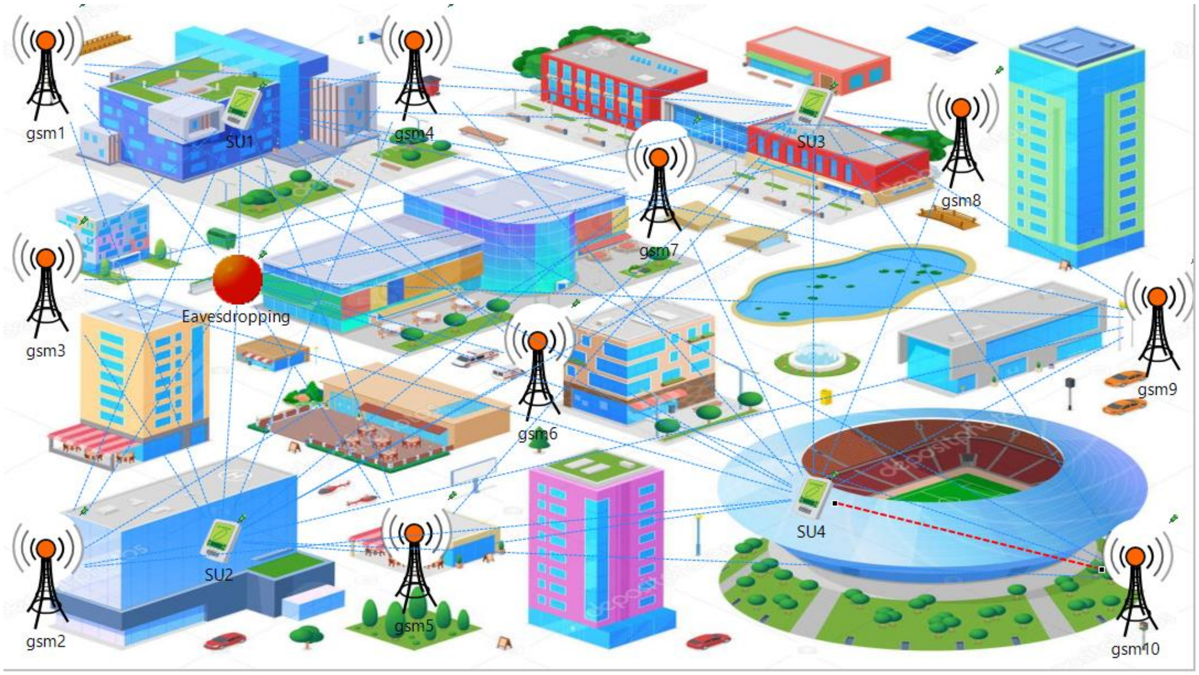


Figure (4.20) CRNs topology in networks cellular with an active eavesdropping attack.

The signals for the application layer, mac layer, and spectrum sensing that are collected interconnection layers (PHY-mac layer) in the transmitter unit are summarized in Table (4-19). The transmission result for the SU1 unit is shown in Figure (4.21).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
AppRequest	**1**	rtsSignal	**1**	sensingSignal	**5.5**

Table (4-19) Application layer request, mac layer and spectrum sensing values.

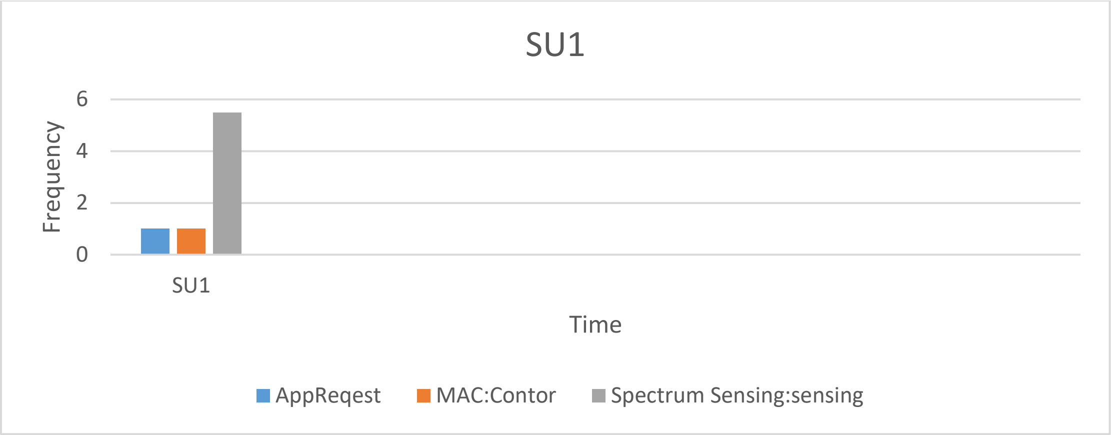


Figure (4.21) statistical results from transmitter SU1 unit

The results for the data and sensing signals in the receiver Req1 unit are summarized in Table (4-20). The receiver unit's results are shown in Figure (4.22).

MAC Layer		**Spectrum Sensing**	
dataSignal	**0**	sensingSignal	**1.8**

Table (4-20) Values from receiver Req1 unit.

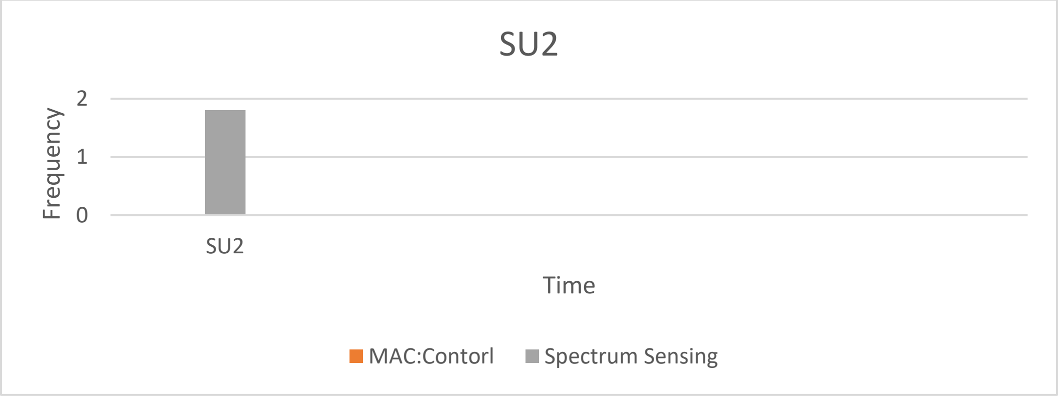


Figure (4.22) Statistical results from Receiver Req1 unit

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-21). (SU3). The transmission result for the (Req2) unit is shown in Figure (4.23).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**1**	sensingSignal	**5.3**

Table (4-21) Application layer request, mac layer and spectrum sensing values.

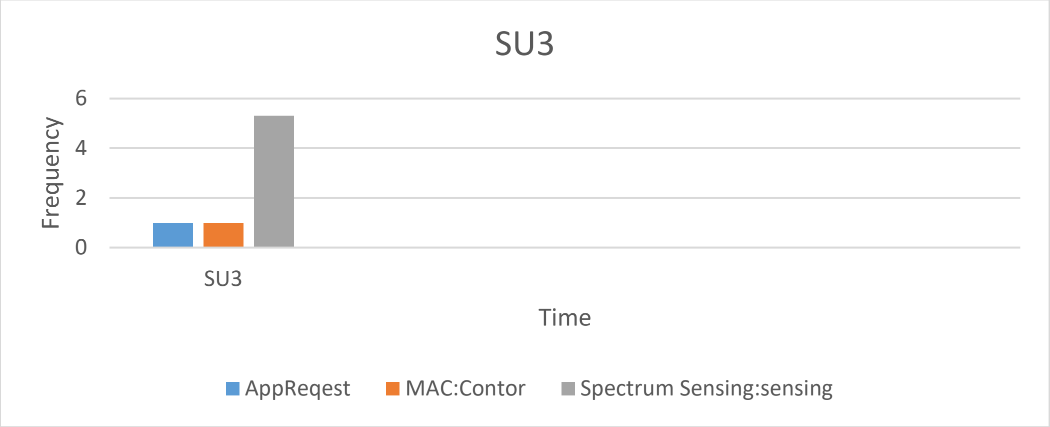


Figure (4.23) Statistical results from Transmitter SU3 unit

Table (4-22) summarizes the results for data signals and sensing signals in the receiver Req2 unit. while Figure (4.24) shows the results statics for the receiver unit.

MAC Layer		**Spectrum Sensing**	
dataSignal	**45**	sensingSignal	**7.1**

Table (4-22) Values from receiver Req2 unit.

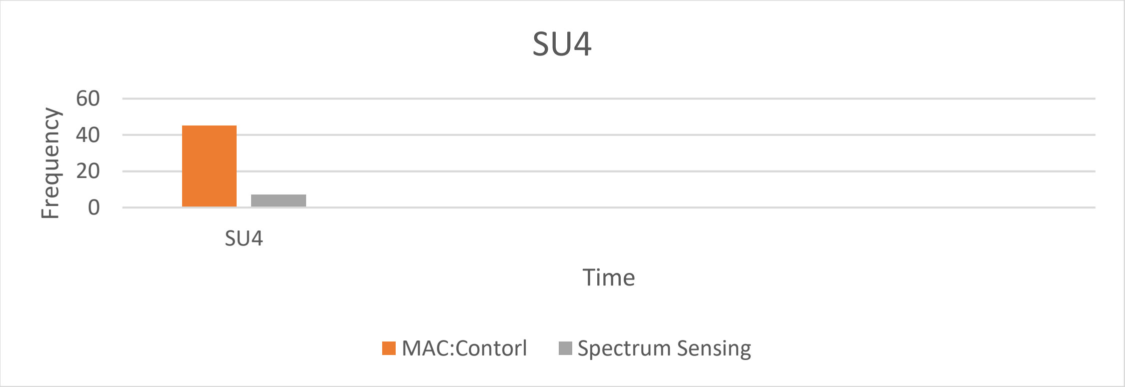


Figure (4.24) Statistical results from Receiver Req2 unit

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-23). (an active eavesdropping attack). The transmission result for the (an active eavesdropping attack) unit is shown in Figure (4.25).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**1**	sensingSignal	**5.3**

Table (4-23) Application layer request, mac layer and spectrum sensing values.

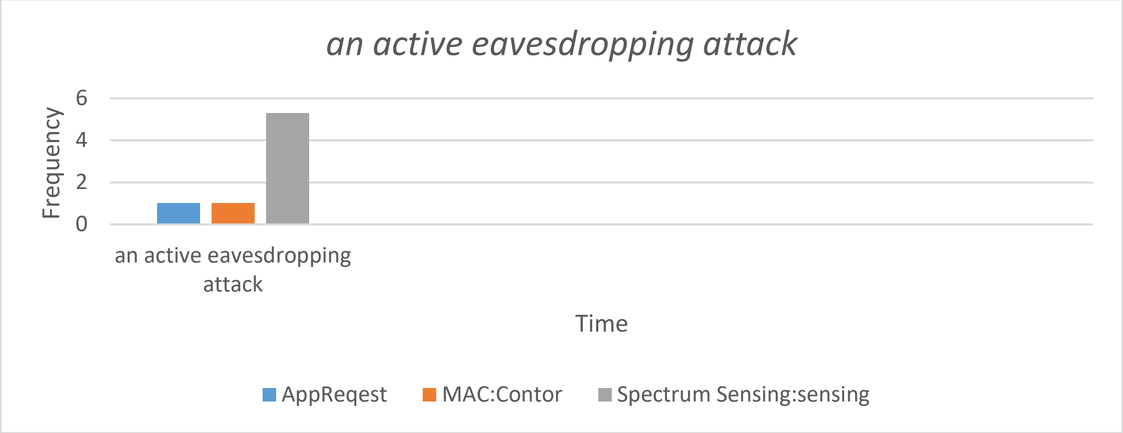


Figure (4.25) Statistical results from Transmitter an active eavesdropping attack unit

Figure (4.26) depicts the difference in data message counts between (SU2 and SU4) receivers. Table (4-24) also demonstrates how to count data signals using receivers.

Receiver	Data Signal (Frames)
SU2	0
SU4	45

Table (4-24) Data Signal for all receivers.

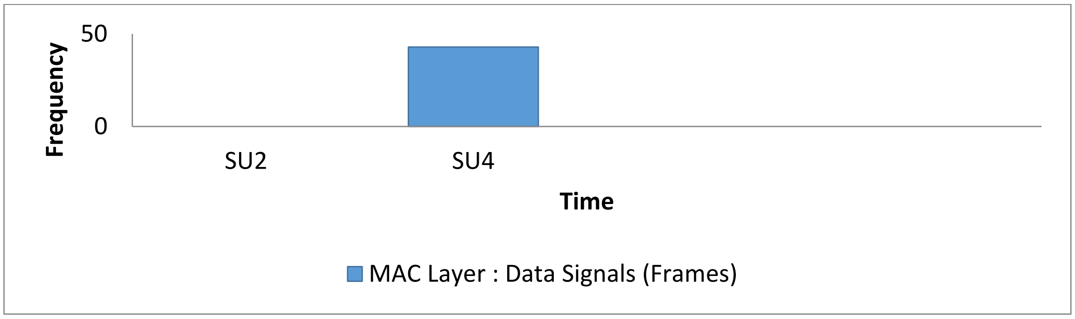


Figure (4.26) Statistical results from all active receiver units.

4.6 Case study of proposed Security of Cognitive Radio Network

The proposed system designed a CRNs in OMNET++ which contains ten primary users and four secondary users, furthermore, each primary user has a licensed PU Base Station (BS) as Global System for Mobile communication (GSM). As well as, the data sources unit described with the initialize keywords which have been entered to the proposed system and their encryption text. Figure (4.27) shows the general network topology and the proposed network cellular in the Cognitive Radio Network.

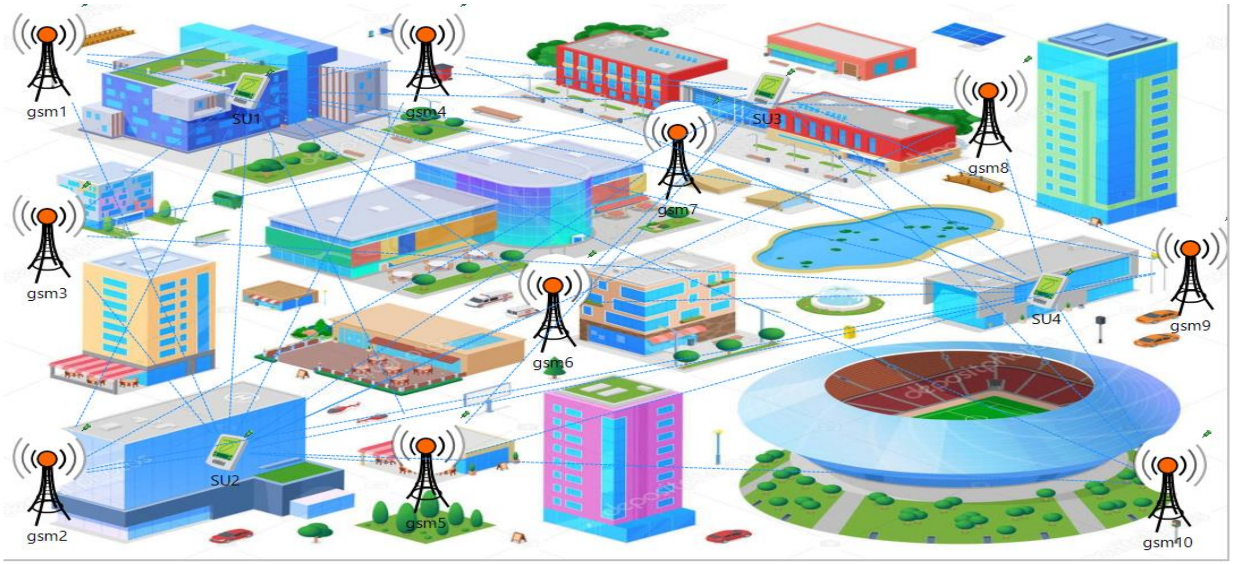


*Figure (4.*27) *The proposed topology of CRNs in networks cellular.*

Simulation states will represent in Figures below to messages exchanged between transmitter and receiver and how they are passing through frequency bands with ten proposed channels while Figure (4.28) represents How messages exchanges between transmitter (SU1) unit and receiver (SU2) unit through the channel 1 when to arrive ACK from the receiver.

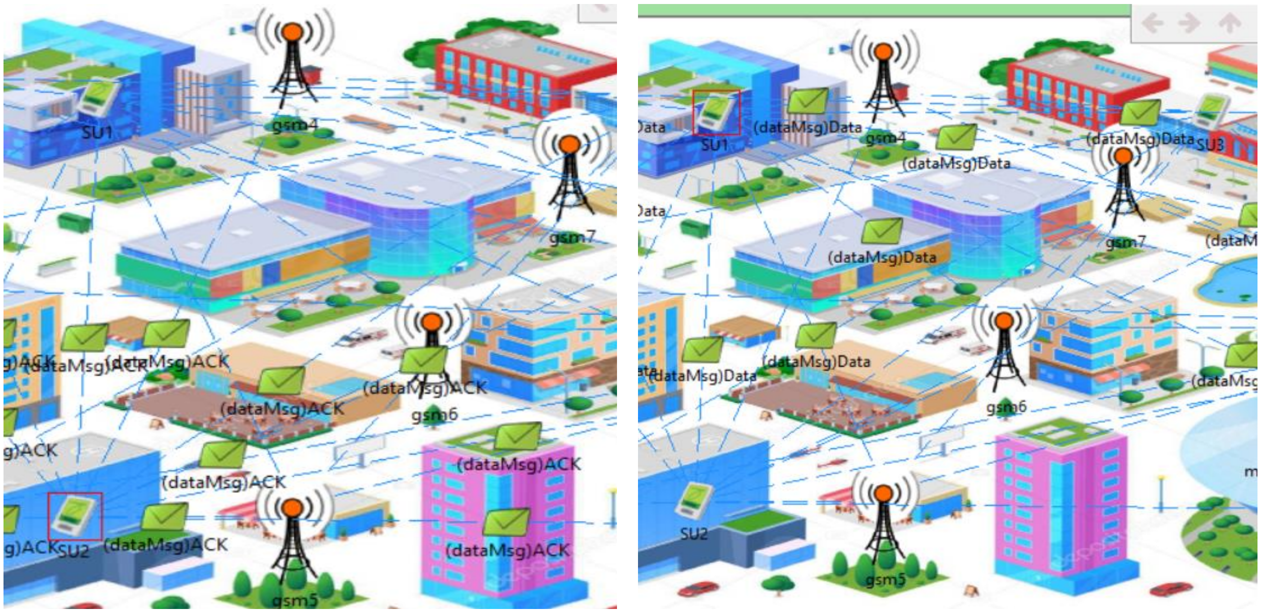


*Figure (4.*28) *ACK request and Data reply message (Data) on the channel 1*

We will illustrate many parameters within the statistical results that will be passed signals between layers and for each transmitter node and receiver node under Layers. These parameters implemented in the main layers that contain algorithms for the proposed system. They are also affected when they go from one node to the next in each case study. Some of the statistics results are explained in Figure (4.29). (application layer request which is helping to get the channel from the primary user, the control information request represent by the RTS control message in the MAC layer, sensing a signal to make the appropriate decision in the spectrum sensor module).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**0.4**	sensingSignal	**1.5**

*Table (4-*25) *Application layer request, mac layer and spectrum sensing values.*

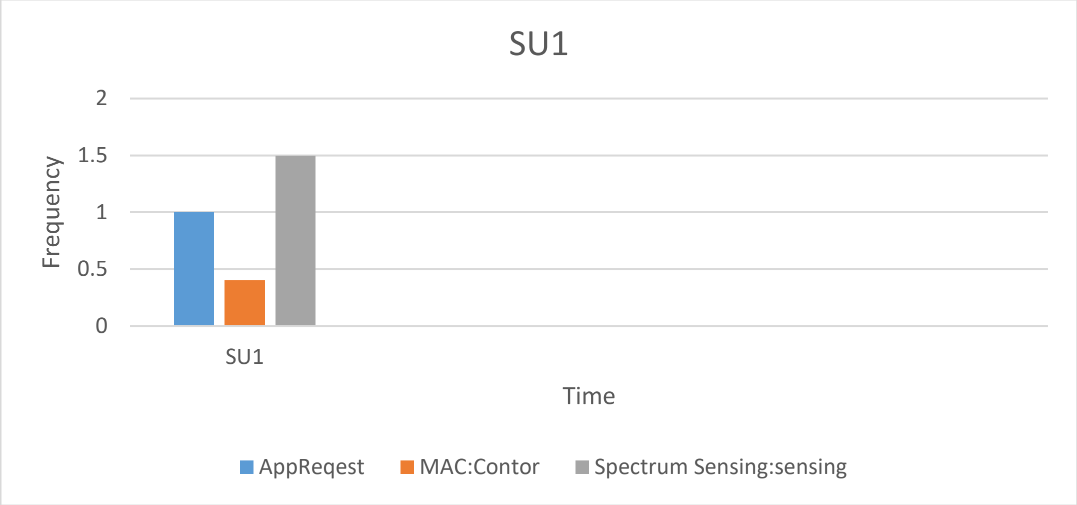


Figure (4.29) Statistical results from Transmitter SU1 unit

The results for the data and sensing signals in the receiver Req1 unit are summarized in Table (4-26). The receiver unit's results are shown in Figure (4.30).

MAC Layer		**Spectrum Sensing**	
dataSignal	**39**	sensingSignal	**1.9**

Table (4-26) Values from receiver Req1 unit.

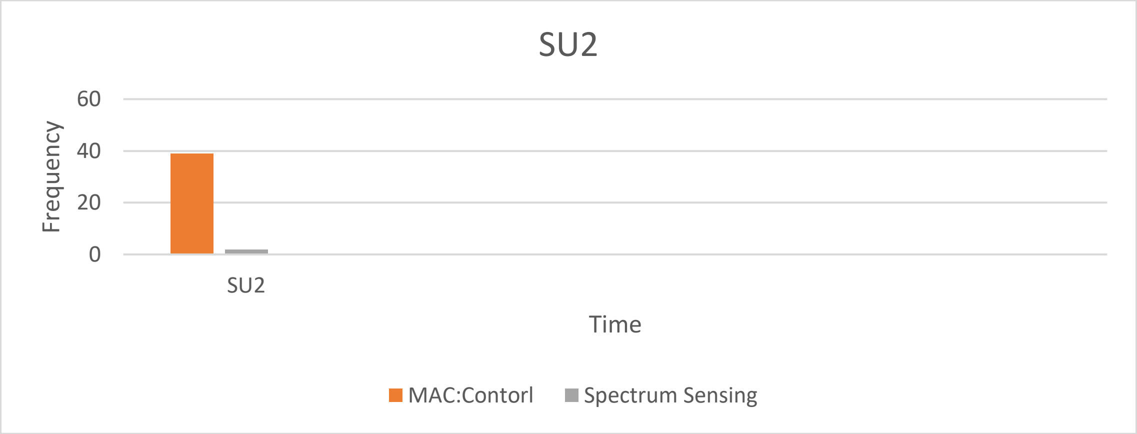


Figure (4.30) Statistical results from Receiver Req1 unit

The signal levels for the application layer, mac layer, and spectrum sensing in the transmitter unit are summarized in Table (4-27). (SU3). The transmission result for the (Req2) unit is shown in Figure (4.31).

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**1**	rtsSignal	**3.9**	sensingSignal	**1.9**

Table (4-27) Application layer request, mac layer and spectrum sensing values.

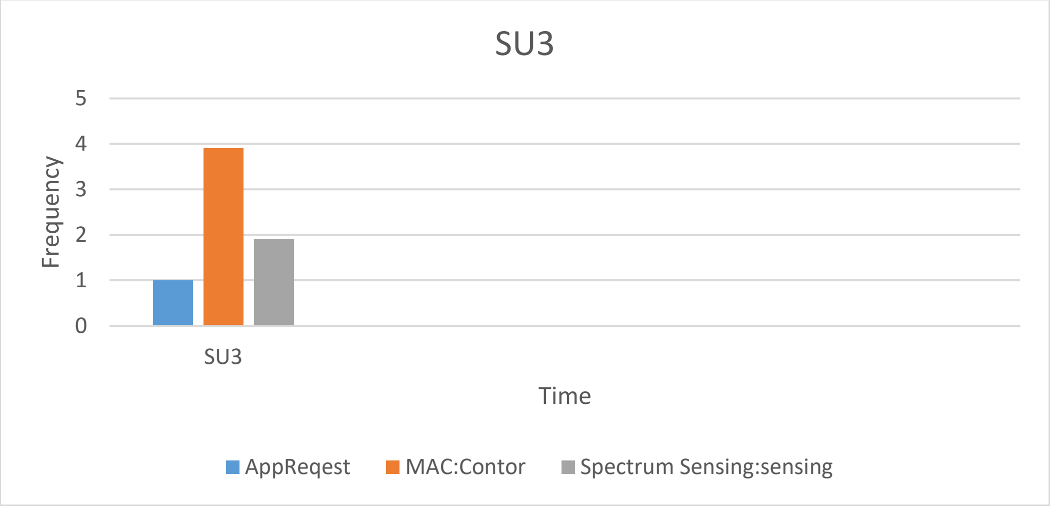


Figure (4.31) Statistical results from Transmitter SU3 unit

Table (4-28) summarizes the results for data signals and sensing signals in the receiver Req2 unit. while Figure (4.32) shows the results statics for the receiver unit.

MAC Layer		**Spectrum Sensing**	
dataSignal	**38**	sensingSignal	**1.9**

Table (4-28) Values from receiver Req2 unit

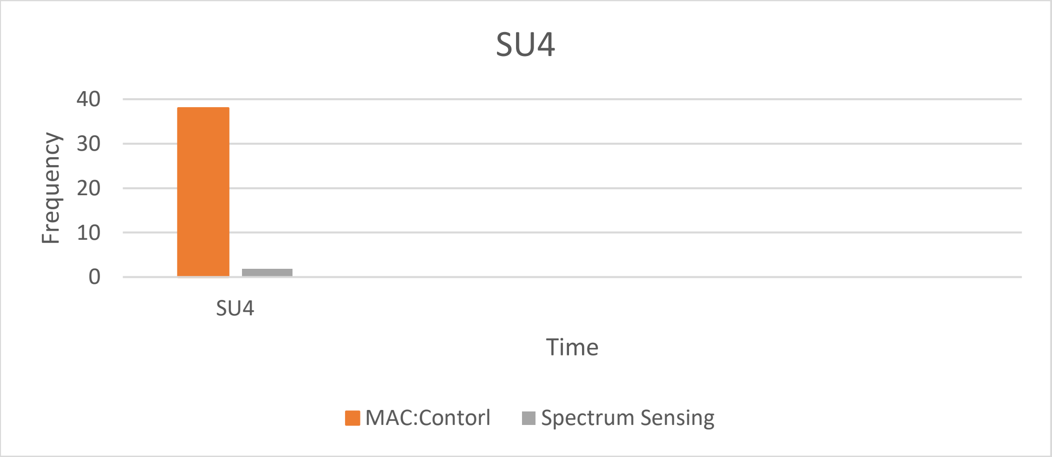


Figure (4.32) Statistical results from Receiver Req2 unit

Figure (4.33) depicts the difference in data message counts between (SU2 and SU4) receivers. Table (4-29) also demonstrates how to count data signals using receivers.

Receiver	Data Signal (Frames)
SU2	39
SU4	38

Table (4-29) Data Signal for all receivers.

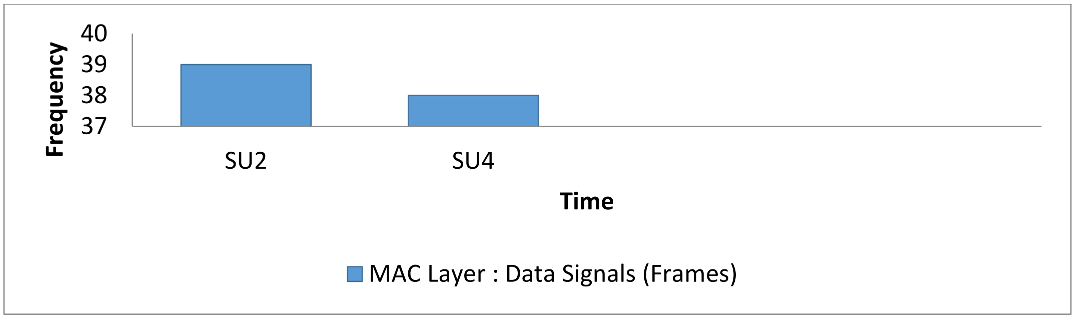


Figure (4.33) Statistical results from all active receiver units.

Figure (4.38) Shows the behaviors of the suggested network elements in a log file.

When comparing the three system states in the state of nature, the state containing an active eavesdropping attack and the protection state using text encryption, the results appear different in all cases, and in the protection state, it is the best as shown in Figure (4.34). And when comparing the two system states, the state in which there is a passive eavesdropping attack with the state against which it was protected, a difference in the results is shown as shown in Figure (4.35).

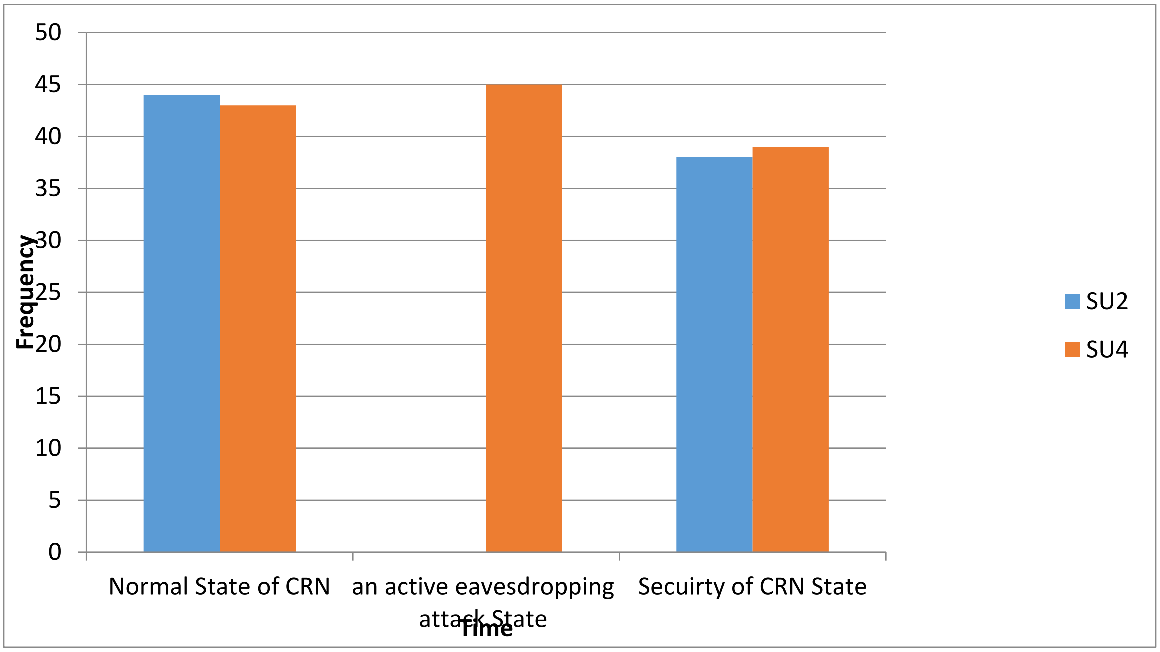


Figure (4.34) Comparisons of three cases studies.

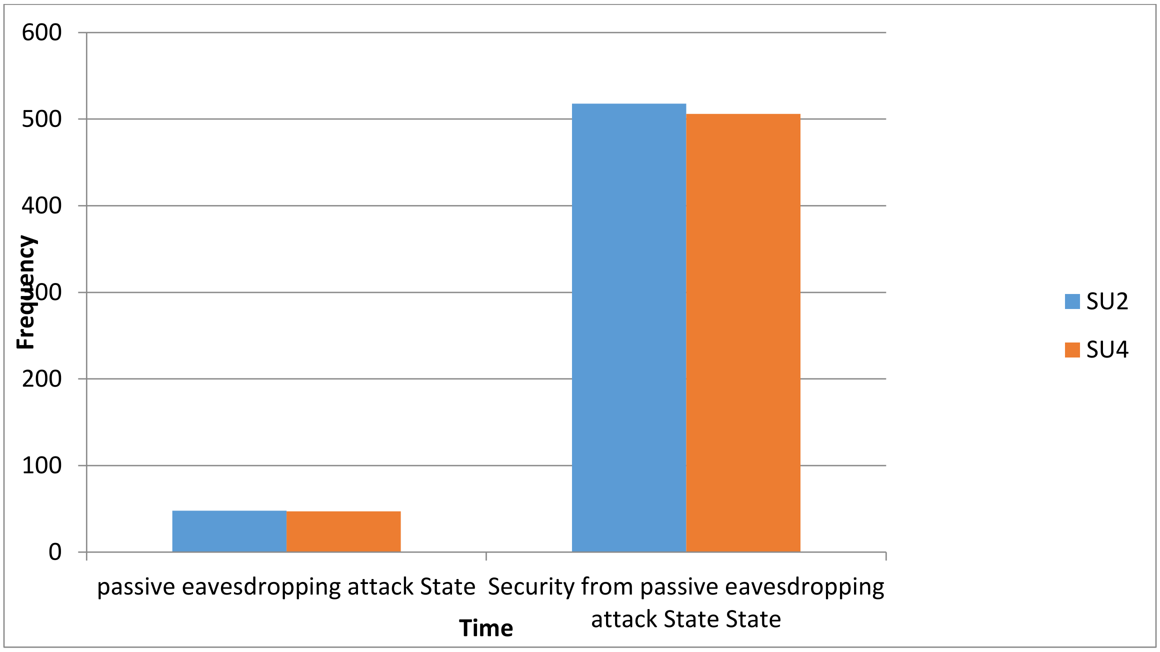


Figure (4.35) Comparisons between passive eavesdropping attack and Protection from passive.

Chapter Five

Conclusions and Future Works

5.1Conclusions

1- Cognitive Radio (CR) technology has been developed to overcome the scarcity of spectrum due to the rapid development of wireless networks. Both authorized and unauthorized users can use spectrum with this technology.

2- The chaotic encryption algorithm is used to protect messages from an active eavesdropping attack because the main advantage is that the chaotic signal appears to unauthorized users as noise, and the chaotic signals are very sensitive to the starting conditions.

3- We can protect data transmitted from passive eavesdropping through that are allow secondary users who know them through their IP addresses to use the empty channels, but any external user over there does not have an IP address it is considered an attack, they are not allowed to use the empty channel.

5.2 Future works

1. Apply the proposed security system to the different application environments, such as battle damage assessments, battlefield surveillance, intelligence assistance, and targeting.

2. Expand the proposed system to include other data kinds including video, audio, and files.

3. Use a different form of attack on a physical layer, or try different types of attack on different layers or functions.

4. A variety of additional encryption algorithms are used to protect networks from the same type of eavesdropping attack.

5. Minimize the use of external frameworks by implementing encryption technology within the same security system.

References

References:

[1] Ji Li "EFFICIENT DISTRIBUTED RENDEZVOUS SCHEMES AND SPECTRUM MANAGEMENT FOR COGNITIVE RADIO NETWORKS" Published by ProQuest LLC (2017).

[2] G. Balakrishnan "COGNITIVE RADIO COOPERATIVE SPECTRUM SENSING", B. E., 2013, B.V. Bhoomaraddi College of Engineering and Technology, India, Published by ProQuest LLC (2017).

[3] G. Sklivanitis, "SOFTWARE-DEFINED ARCHITECTURES FOR SPECTRALLY EFFICIENT COGNITIVE NETWORKING IN EXTREME ENVIRONMENTS", A dissertation submitted to the Faculty of the Graduate School of the University at Buffalo, State University of New York, Published by ProQuest LLC (2018).

[4] C. Ran, "Spectrum Sharing in Large-Scale and Random Geometric Wireless Networks", A Thesis Submitted in Partial Fulfillment, Published by ProQuest LLC (2015).

[5] H. Mohammad Almasaeid, "Spectrum allocation algorithms for cognitive radio mesh networks",2012 by ProQuest LLC.

[6] Y. SHENG SHIU AND SHIH YU CHANG, HSIAO-CHUN WU, HSIAO-HWA CHEN, "PHYSICAL LAYER SECURITY IN WIRELESS NETWORKS", IEEE Wireless Communications • April 2011.

[7] S. Zhuhai; Qian, Yi; and Ci, Song, "On Physical Layer Security for Cognitive Radio Networks" (2013). Faculty Publications from the Department of Electrical and Computer Engineering. 346.

[8] Y, Wang, L, Zaidi, SAR et al. "Artificial-Noise Aided Secure Transmission in Large Scale Spectrum Sharing Networks". IEEE Transactions on Communications, 64 (5). pp. 2116-2129. ISSN 0090-6778, (2016).

[9] Y. Zou, Jia Zhu, Xianbin Wang, and Victor C.M. Leung," Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques"arXiv:1405.3725v1 [cs. IT] 15 May 2014.

References

[10] G. Geraci, Harpreet S. Dhillon, Jeffrey G. Andrews, Jinhong Yuan, and Iain B. Collings, "Physical Layer Security in Downlink Multi-Antenna Cellular Networks", IEEE Transactions on Communications · July 2013, DOI: 10.1109/TCOMM.2014.2314664 · Source: arXiv.

[11] G. Tiwari Debashis Nandi Madhusudhan Mishra, "Chaotic Cryptography and Multimedia Security: A Review", International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 10, October - 2013.

[12] B.Li, Xiaohui Qi, Kaizhi Huang, Zedong Fei, Fuhui Zhou, and Rose Qingyang Hu, "Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 67, NO. 1, JANUARY 2019.

[13] Y. Jiang, Yulong Zou, Jian Ouyang, and Jia Zhu, "Secrecy Energy Efficiency Optimization for Artificial Noise Aided Physical-Layer Security in OFDM-Based Cognitive Radio Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (ACCEPTED TO APPEAR), arXiv:1810.05119v1 [cs.IT] 11 Oct 2018.

[14] K. Ho-Van and Thiem Do-Dac, "Reliability-Security Trade-Off Analysis of Cognitive Radio Networks with Jamming and Licensed Interference", Hindawi, Wireless Communications and Mobile Computing Volume 2018, Article ID 5457176, 15 pages.

[15] M. Harun YJlmaz, ErtuLrul Güvenkaya, Haji M. Furqan, Selçuk Köse, and Hüseyin Arslan, "Cognitive Security of Wireless Communication Systems in the Physical Layer", Hindawi Wireless Communications and Mobile Computing Volume 2017, Article ID 3592792, 9 pages.

[16] H. Al-Hraishawi, Gayan Amarasuriya Aruma Badge, and Rafael F. Schaefer, "Artificial Noise-Aided Physical Layer Security in Underlay Cognitive Massive MIMO Systems with Pilot Contamination", MDPI, Entropy 2017, 19, 349; doi:10.3390/e19070349.

[17] Y. Cai, Xiaoping Xu, Weiwei Yang, "Secure transmission in the random cognitive radio networks with secrecy guard zone and artificial noise", IET Communications, DOI: 10.1049/it-com.2016.0117 www.ietdl.org.

References

[18] A. El Shafie, Dusit Niyato, Naofal Al-Dhahir, "Artificial-Noise-Aided Secure MIMO Full-Duplex Relay Channels with Fixed-Power Transmissions", DOI 10.1109/LCOMM.2016.2579623, IEEE Communications Letters.

[19] B. Fang, Zuping Qian, Wei Shao, and Wei Zhong, "Joint Precoding and Artificial Noise Design for Cognitive MIMOME Wiretap Channels", DOI 10.1109/TVT.2015.2477305, IEEE Transactions on Vehicular Technology.

[20] A. NASR," A NOISE ESTIMATION SCHEME FOR BLIND SPECTRUM SENSING USING EMD", Published by ProQuest LLC (2017).

[21] S. Dekate, "STUDY OF DYNAMIC SUBCARRIER COORDINATE INTERLEAVING FOR EAVESDROPPING PREVENTION IN ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING SYSTEMS"B. E, 2013, Lokmanya Tilak College of Engineering, Mumbai, India December 2015.

[22] T. Akitaya, Shunta Asano, and Takahiko Saba, "Time-domain Artificial Noise Generation Technique Using Time-domain and Frequency-domain Processing for Physical Layer Security in MIMO-OFDM Systems", Dept. of Computer Science, Chiba Institute of Technology, 2-17-1 Tsudanuma, Narashino, Chiba 275-0016 JAPAN, DOI: 10.1109/ICCW.2014.6881299.

[23] L. Safety, Mario Bkassiny, Mohammed Al-Husseini, and Ali El-Hajj, "Cognitive Radio Transceivers: RF, Spectrum Sensing, and Learning Algorithms Review", Hindawi Publishing Corporation International Journal of Antennas and Propagation Volume 2014, Article ID 548473, 21 pages.

[24] S. LIEN, "COGNITIVE RADIO RESOURCE MANAGEMENT FOR FUTURE CELLULAR NETWORKS", IEEE Wireless Communications • February 2014.

[25] J. Zhu, "Security-reliability trade-off for cognitive radio networks in the presence of eavesdropping the attack", Zhu EURASIP Journal on Advances in Signal Processing 2013, 2013:169.

[26] V. Tam Nguyen, Frederic Villain, and Yann Le Guillen, "Cognitive Radio RF: Overview and Challenges", Hindawi Publishing Corporation VLSI Design Volume 2012, Article ID 716476, 13 pages doi:10.1155/2012/716476.

References

[27] J. Sen, "Security and Privacy Challenges in Cognitive Wireless Sensor Networks", Innovation Lab, Tata Consultancy Services Ltd., Kolkata, India 2011.

[28] I. F. Akyildiz, Brandon F. Lo, Ravikumar Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey", Physical Communication 4 (2011) 40–62, journal homepage: www.elsevier.com/locate/phycom.

[29] D. Goeckel, Sudarshan Vasudevan, Don Towsley, Stephan Adams, Z. Ding, and K. Leung,"Dennis Goeckel, Sudarshan Vasudevan, Don Towsley, Stephan Adams, Z. Ding, and K. Leung" Artificial Noise Generation from Cooperative Relays for Everlasting Secrecy in Two-Hop Wireless Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 10, DECEMBER 2011.

[30] S. Yaw Nusenu, "Authentication and Secrecy of Multicast Communication Scenario: Artificial Noise-Aided Costas Sequence Matrix FDA Approach", Hindawi Security and Communication Networks Volume 2020, Article ID 2194840, 13 pages.

[31] H. Lu, Lin Zhang, Ming Jiang, and ZhiqiangWu, "High-Security Chaotic Cognitive Radio System with Subcarrier Shifting", IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 10, OCTOBER 2015.

[32] L. Zhang · Huaiyin Lu· ZhiqiangWu · Ming Jiang,"Bit error rate analysis of chaotic cognitive radio system over slow fading channels", Ann. Telecomm. (2015) 70:513–521 DOI 10.1007/s12243-015-0472-9.

[33] H. Hassani, Nader Alharbi and Mansi Ghodsi,"Distinguishing chaos from noise: A new approach", International Journal of Energy and Statistics Vol. 2, No. 2 (2014) 137–150, Institute for International Energy Studies DOI: 10.1142/S2335680414500100.

[34] H. N. Abdullah and Alejandro A. Valenzuela, "Efficient Chaotic Communication System for Wireless Sensing Applications",2012 – 9th International Multi-Conference on Systems, Signals and Devices.

[35] B. R. Ivan and S. D. Dhodapkar, "CHAOS BASED CRYPTOGRAPHY: A NEW APPROACH TO SECURE COMMUNICATIONS"BARC NEWSLETTER. 258 July 2005.

References

[36] G. Alvarez and Shujun Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems", International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006.

[37] M. Farajallah, "Chaos-based crypto and joint crypto-compression systems for images and videos", HAL Id: tel-01179610 https://hal.archives-ouvertes.fr/tel 01179610 Submitted on 23 Jul 2015.

[38] S. Benazzouza, Mohammed Redound, Fatima Salahdine, and Aawatif Hayar, "Chaotic Compressive Spectrum Sensing Based on Chebyshev Map for Cognitive Radio Networks", Cognitive Radio Networks. Symmetry 2021, 13, 429. https://doi.org/ 10.3390/sym13030429.

[39] J. Webster (ed.)," AN OVERVIEW OF COGNITIVE RADIO NETWORKS", Wiley Encyclopedia of Electrical and Electronics Engineering.DOI: 10.1002/047134608X.W8355,2017.

[40] Y. Song, "DISTRIBUTED INTELLIGENT SPECTRUM MANAGEMENT IN COGNITIVE RADIO AD HOC NETWORKS" Published by ProQuest LLC (2013).

[41] Z. Ping, LIU Yang, FENG Zhi-Yong, ZHANG QiXun, LI Qian & XU Ding, "Intelligent and efficient development of wireless networks: A review of cognitive radio networks", Chinese Science Bulletin, October 2012 Vol.57 No.28-29: 36623676, doi: 10.1007/s11434-012-5334-5.

[42] T. Mukherjee Asoke Nath, "Cognitive Radio Network Architecture and Security Issues: A Comprehensive Study", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 6, June 2015.

[43] A. K. M. Muzahidul Islam · Mahdi Zareei ·Sabariah Baharun · Toshio Wakabayashi · Shozo Komaki, "Cognitive Radio Ad-Hoc Network Architectures: A Survey", Wireless Pers Commun, DOI 10.1007/s11277-014-2175-3, Springer,2014.

[44] C. Wu, "Novel Function Approximation Techniques for Large-scale Reinforcement Learning", ProQuest LLC 789 East Eisenhower Parkway,2011.

[45] M. Ali Shah, Sijing Zhang, Muhammad Kamran, Qaisar Javaid, and Bahjat Fatima, "A survey on MAC protocols for complex self-organizing cognitive radio

networks", Shah et al. Complex Adapt System Model (2016) 4:18, DOI 10.1186/s40294-016-0030-y.

[46] X. Zhou and Matthew R. McKay, "Physical Layer Security with Artificial Noise: Secrecy Capacity and Optimal Power Allocation", Authorized licensed use limited to Australian National University. Downloaded on November 14, 2009, from IEEE Xplore. Restrictions apply.

[47] M. Khasawneh, Anjali Agarwal,"A Survey on Security in Cognitive Radio Networks",2014 6th International Conference on CSIT.

[48] S. Bhagavathy Nanthini, M. Hemalatha, D. Manivannan, and L. Devasena," Attacks in Cognitive Radio Networks (CRN)A Survey", Indian Journal of Science and Technology, Vol 7(4), 530–536, April 2014.

[49] X. Chen and Michael R. Lyu,"Reliability Analysis for Various Communication Schemes in Wireless CORBA", IEEE TRANSACTIONS ON RELIABILITY, VOL. 54, NO. 2, JUNE 2005.

[50] C. Maple, Geraint Williams and Yong Yue, "Reliability, Availability and Security of Wireless Networks in the Community", Research Gate, Informatics 31 (2007) 201–208 201

[51] N. Mathur and K. P. Subbalakshmi, "Security Issues in Cognitive Radio Networks", Qusay H. Mahmoud c11.tex V1 - April 24, 2007.

[52] A. AL-TALABANI," ENHANCING PHYSICAL LAYER SECURITY IN COGNITIVE RADIO NETWORKS", KING'S COLLEGE LONDON 2016.

[53] M. H. Khan, P.C. Barman, "Analysis of Attacks in Cognitive Radio Networks", American Journal of Engineering Research (AJER) 2016.

[54] M. Riahi Manesh and Naima Kaabouch, "Security Threats and Countermeasures of MAC Layer in Cognitive Radio Networks", Article in Ad Hoc Networks · November 2017 DOI: 10.1016/j.adhoc.2017.11.003.

[55] M. Padmadas, Dr.N. Krishnan, Vanilla Nayaki, "Analysis of Attacks in Cognitive Radio Networks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015.

References

[56] Yulong Zou, Jia Zhu, Liuqing Yang, Ying-Chang Liang, and Yu-Dong Yao," Securing Physical-Layer Communications for Cognitive Radio Networks", arXiv:1507.00598v1 [cs.IT] 2 Jul 2015.

[57] W. Alhakami, "Secure MAC Protocols for Cognitive Radio Networks", Department of Computer Science and Technology University of Bedfordshire January 2016.

[58] Y. Zhang • Jijun Luo • Honglin Hu," WIRELESS MESH NETWORKING", Auerbachian Publications is an imprint of the Taylor & Francis Group, an Informal business,2007.

[59] M. KHASAWNEH AND ANJALI AGARWAL, "A Secure and Efficient Authentication Mechanism Applied to Cognitive Radio Networks", IEEE, current version August 22, 2017. Digital Object Identifier 10.1109/ACCESS.2017.2723322.

[60] S. Parvin, "Trust-based Mechanisms for Secure Communication in Cognitive Radio Networks", School of Information Systems, Curtin Business School Curtin Universit,2013.

[61] I. Yasser, Mohamed A. Mohamed, Ahmed S. Samra, and Fahmi Khalifa,"A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications"MDPI, Published: 4 November 2020.

[62] M. Y T Irsan, and S C Antonio, "Text Encryption Algorithm based on Chaotic Map", Journal of Physics: Conference Series 1341 (2019) 062023, doi:10.1088/1742-6596/1341/6/062023.

[63] A. Akg¨ul, Sezgin Kac¸ar, Burak Arıcıo˘glu, ˙Ihsan Pehlivan, "Text Encryption by Using One-Dimensional Chaos Generators and Nonlinear Equations, "ResarchGate, Conference Paper · November 2013, DOI: 10.1109/ELECO.2013.6713853.

[64] D. Houcque, "INTRODUCTION TO MATLAB FOR ENGINEERING STUDENTS", Northwestern University (August 2005).

[65] T. Issariyakul • Ekram Hossain,"Introduction to Network Simulator NS2", DOI 10.1007/978-1-4614-1406-3, Springer New York Dordrecht Heidelberg London, LLC 2012.

References

[66] A. Varga and Rudolf Hornig," AN OVERVIEW OF THE OMNeT++ SIMULATION ENVIRONMENT", SIMUTools, March 03 – 07, 2008, Marseille, France. ISBN 978-963-9799-20-2.

[67] B. Krupanek and Ryszard Bogacz, "OPNET Modeler simulations of performance for multi-nodes wireless systems", EDP Sciences, Int. J. Metrol. Qual. Eng. 7, 105 (2016).

[68]https://www.google.com/search?q=frequency+utilization+of+primary+and+secondary+users+in+cognitive+radio+environment&source=lnms&tbm=isch&sa=X&ved=2ahUKEwi6r5WGm7n0AhWJ7rsIHb0SAIwQ_AUoAXoECAEQAw&biw=1536&bih=754&dpr=1.25

[69]https://www.google.com/search?q=passive+attack&source=lnms&tbm=isch&sa=X&ved=2ahUKEwj2iOnom7n0AhXSgP0HHRv4AQMQ_AUoAXoECAEQAw&biw=1536&bih=754&dpr=1.25#imgrc=P8YkFTiuOrkYxM

[70]https://www.google.com/search?q=active+attack&tbm=isch&ved=2ahUKEwifyIrsm7n0AhUOdRQKHWfxAl0Q2cCegQIABAA&oq=active+attack&gs_lcp=CgNpbWcQAzIECAAQQzIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABFCAB1ipFWD7G2gAcAB4BIAB_wOIAfMTkgELMC4xLjIuMC4zLjGYAQCgAQGqAQtnd3Mtd2l6LWltZ7ABAMABAQ&sclient=img&ei=8X6iYd-LJ47qUefii-gF&bih=754&biw=1536#imgrc=IZQ8O7fpjgglTM

[71]https://www.google.com/search?q=the+major+functions+for+the+CR+networks&tbm=isch&ved=2ahUKEwiJ5LKvnLn0AhUCjqQKHbK5D5wQ2-cCegQIABAA&oq=the+major+functions+for+the+CR+networks&gs_lcp=CgNpbWcQAzoECAAQQzoFCAAQgARQuwZYsxRgkhtoAHAAeASAAdwFiAHSHZIBCTMtMS4yLjMuMZgBAKABAaoBC2d3cy13aXotaW1nsAEAwAEB&sclient=img&ei=fniYYmtMYKckgWy877gCQ&bih=754&biw=1536#imgrc=8JYX6Ad_jEFtQM

[72]https://www.google.com/search?q=behavior+of+Primary+and+secondary+users+&tbm=isch&ved=2ahUKEwj5jI3Vqrn0AhXhgqQKHekqA6wQ2cCegQIABAA&oq=behavior+of+Primary+and+secondary+users+&gs_lcp=CgNpbWcQA1AAWABgpAZoAHAAeACAAcIBiAHCAZIBAzAuMZgBAKABAaoBC2d3cy13aXotaW1nwAEB&sclient=img&ei=e46iYbnjOGFkgXp1YzgCg&bih=754&biw=1536

References

[73]https://www.google.com/search?q=the+RTS+Frame+Format+&tbm=isch&ved=2ahUKEwjv1KnpqLn0AhUaNuwKHXXSCqwQ2cCegQIABAA&oq=the+RTS+Frame+Format+&gs_lcp=CgNpbWcQA1CE3QdYhN0HYIrjB2gAcAB4AIABhwSIAYQHkgEJMC4xLjEuNS0xmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=jYyiYa_aH5rssAf1pKvgCg&bih=754&biw=1536#imgrc=y3lb4TL4trcV1M&imgdii=7itf8NITFBd23M

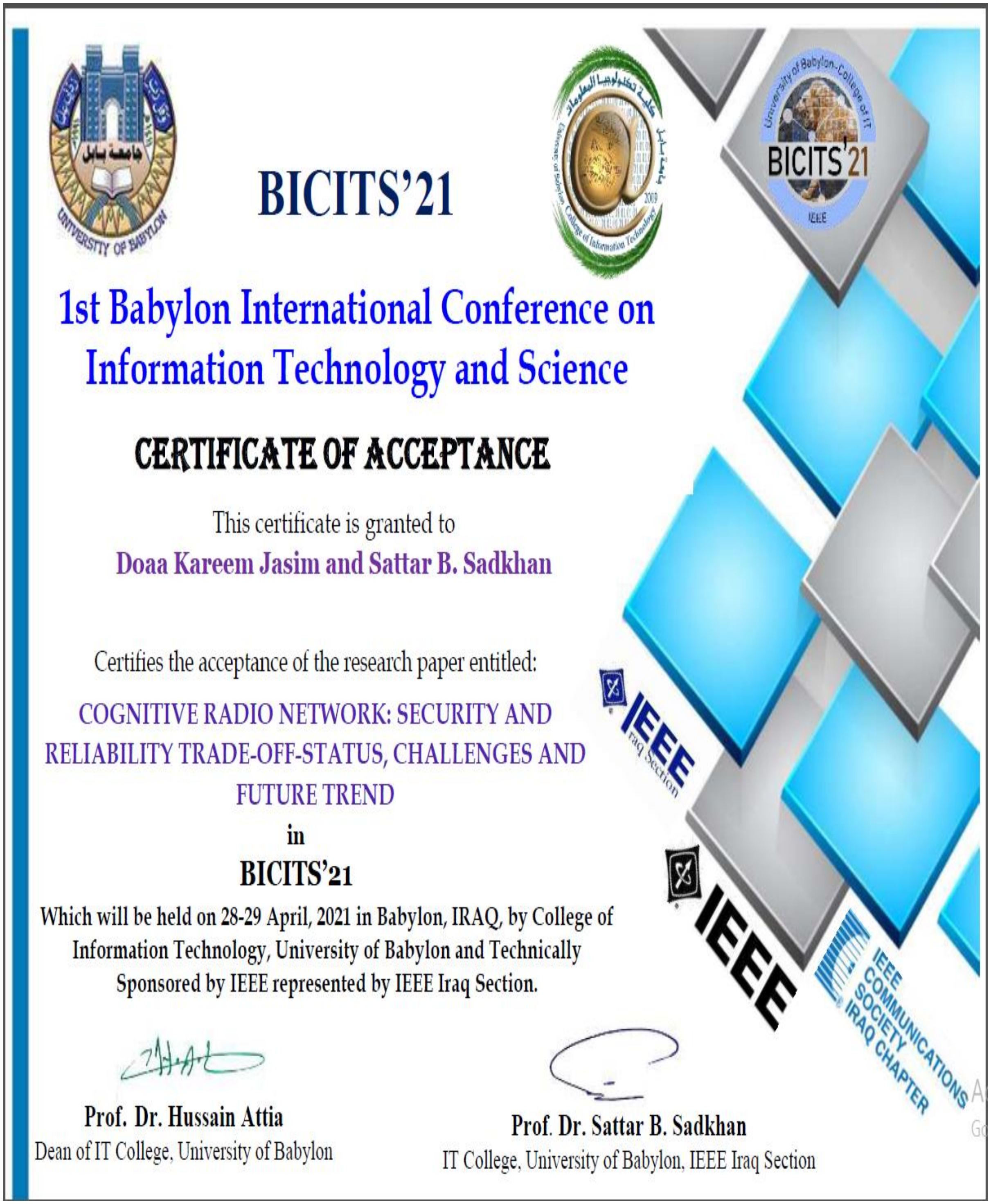
[74]https://www.google.com/search?q=the+CTS+Frame+Format&tbm=isch&ved=2ahUKEwix9ayzqbn0AhXO0AKHcarDOYQ2cCegQIABAA&oq=the+CTS+Frame+Format&gs_lcp=CgNpbWcQA1AAWABgpgZoAHAAeACAAZQCiAGUApIBAzItMZgBAKABAaoBC2d3cy13aXotaW1nwAEB&sclient=img&ei=KI2iYbHBLs6ngwfG17KwDg&bih=754&biw=1536#imgrc=y3lb4TL4trcV1M

[75]https://www.google.com/search?q=the+Acknowledgement+Frame+Format+&tbm=isch&ved=2ahUKEwjW9aaQqrn0AhUHDhQKHcL5BjMQ2-cCegQIABAA&oq=the+Acknowledgement+Frame+Format+&gs_lcp=CgNpbWcQA1DnCljnCmCEWgAcAB4AIAB2gGIAY8DkgEFMC4xLjGYAQCgAQGqAQtnd3Mtd2l6LWltZ8ABAQ&sclient=img&ei=642iYZbUKoecUMLzm5gD&bih=754&biw=1536#imgrc=muqziPBiiMVQxM

[76] A. Sameer Hamood, Sattar B. Sadkhan "Keywords Sensitivity Recognition of Military Applications in Secure CRNs Environments", 2017 Second Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), 2017.

Appendix

Appendix A



BICITS'21

1st Babylon International Conference on Information Technology and Science

CERTIFICATE OF ACCEPTANCE

This certificate is granted to

Doaa Kareem Jasim and Sattar B. Sadkhan

Certifies the acceptance of the research paper entitled:

COGNITIVE RADIO NETWORK: SECURITY AND RELIABILITY TRADE-OFF-STATUS, CHALLENGES AND FUTURE TREND

in

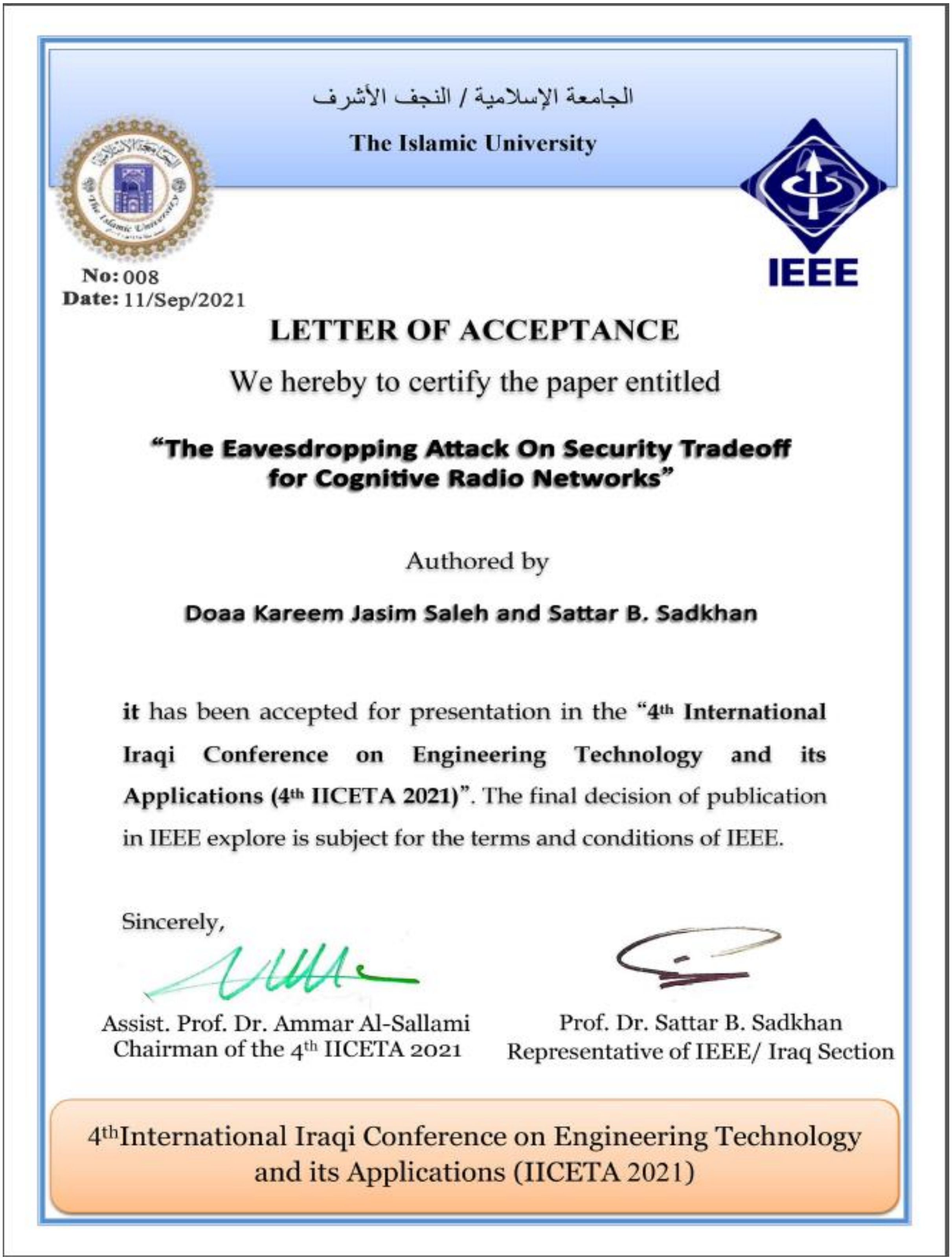
BICITS'21

Which will be held on 28-29 April, 2021 in Babylon, IRAQ, by College of Information Technology, University of Babylon and Technically Sponsored by IEEE represented by IEEE Iraq Section.

Prof. Dr. Hussain Attia
Dean of IT College, University of Babylon

Prof. Dr. Sattar B. Sadkhan
IT College, University of Babylon, IEEE Iraq Section

Appendix



الجامعة الإسلامية / النجف الأشرف

The Islamic University

IEEE

No: 008
Date: 11/Sep/2021

LETTER OF ACCEPTANCE

We hereby to certify the paper entitled

"The Eavesdropping Attack On Security Tradeoff for Cognitive Radio Networks"

Authored by

Doaa Kareem Jasim Saleh and Sattar B. Sadkhan

it has been accepted for presentation in the **"4th International Iraqi Conference on Engineering Technology and its Applications (4th IICETA 2021)"**. The final decision of publication in IEEE explore is subject for the terms and conditions of IEEE.

Sincerely,

Assist. Prof. Dr. Ammar Al-Sallami
Chairman of the 4th IICETA 2021

Prof. Dr. Sattar B. Sadkhan
Representative of IEEE/ Iraq Section

4thInternational Iraqi Conference on Engineering Technology and its Applications (IICETA 2021)

Appendix B

Appendix B explained the layer of omnet++ and show what the meant every layer and function every layer.

1) Application layer: no actual data is sent. Instead, it uses the layers below to deliver a request to the MAC layer. The MAC Layer generates a random number of data packets (as specified in the.ini file) that affect the simulation's overall performance. As a result, files can be used to hold parameters that are expected to change (or should change) during research.) and tries to send it to a certain location. It also generates random numbers of transmission data based on the configuration file's settings. Furthermore, based on the signaling function, it gathers statistics on effective and unsuccessful contact.

Appendix

The proposed system used a series of parameters to replicate the application layer's general function in a cognitive radio network.

Application Layer Steps: -

Signals from the lower layers are used as input and output.

Step 1: Initialize case, which is defined by:

1- Make the decision to begin a new correspondence situation.

2- Obtaining a list of neighbors.

3- Compiling Statistics

Step 2: Begin using the roles of the Handlers

1- Begin a new conversation.

2- sending a message to the lower layer for the RTS packet to be sent.

3-Controlling Information exchanges.

4- dialing to initiate a conversation

5- the data module for receiving signal messages.

6- dealing with acknowledgment packets

7- sending the CTRL message to the lower layers

8- DATA message routing for lower layers

2)Network layer: chooses a random destination node in the network from its one-hop peer nodes. The one-hop neighbors' addresses must be included in the network's topology (. NED) register.

The network layer deals with upper and lower layer control and data, as well as packet routing via interfaces to decide packet destinations. Inside (crNetLayer.cc and crNetLayer.h) files.

Network Layer Steps

Signals from the lower and upper layers are used as input and output.

Step 1: Create the case, which is defined by: obtaining a list of neighbors.

Step 2: Begin Functions of Handlers

1- Use a special interface to redirect signals from lower/upper layers as control signals and data messages (frames) from lower/upper layers.

3)CR_MAC_Layer: In addition to the mobility function, the medium access management team is responsible for responsibilities such as smart behavior for choosing spectrum bands and encapsulating frames for security reasons. Furthermore, have exclusive capabilities not present in conventional wireless networks. Via dynamic channel accessibility and channel handoff/handover mechanisms with spectrum sensing, information about the events of available channels was given, and the best channel for communication was selected based on a collection of parameters that determine the CR-MAC protocol's performance. In addition, the proposed scheme used a MAC protocol based on CSMA (RTS, CTS) with channel dynamic control. Many parameters of this configurable protocol may be changed through the configuration file.

CR MAC Layer deals with data types received from the physical layer and passes them to the network layer's [send ()] process, which is used to send messages using various steps. All processes inside (cr80211b.cc, cr80211b.h, crMacLayer.cc and crMacLayer.h) files.

Algorithm for the CR-MAC Layer

Step 1: Create a case that includes frames number, the actual Destination, the present Data Channel, and the proposed Channel.

Step 2: Begin using the roles of the Handlers

1)Handle RTS: if (isTransmitting and isReceiving) are both true, then remove the message; otherwise, "I'm idle and want to perceive the proposed channel" is displayed.

2) Handle CTS: A node's idle state can be restored by clearing an RTS trigger:

data to be sent across the proposed channel

3)Handle Data: The proposed channel starts transmitting after receiving the values for the source, destination, and the number of packets (ack, dataLower). If (ackEnabled == true && currentDataChannel = 0) if not, erase the message

4)Handle Ask: Send frame reset attempts and a simple ACK Timeout Timer for the following packet.

channel is lost, don't send next packet else send next packet. if (currentDataChannel == 0)

5)Hadle Nack: Sensing a free channel and transmitting RTS on that channel was suggested.

(10 channel frequency band by FHSS)

6)Handle PU: If isTransmitting == true, then PU START and END handle the message. I was transmitting and entered with

Two Case: -

Case 1: If (akEnabled== true) {cancel the PU transmission channel, prepare RTS/CTS for the new channel using sense Request(SenseFreeCHANNEL)}

else {Stop issuing acknowledgments until all approved users' transmissions have been completed.}}

Case 2: else {get Idle received, licensed user handover channel}

*/ Handler-dependent functions are those that rely on the presence of a handler.

Sense Request: This functionality is useful for sensing suggested channels as idle in handling RTS, in handling Ack data channels, and in handling PU messages for free channels.

/// Timers

1)*When RTS is sent, the set* ***RTS timer*** *is invoked.*

2)*A node's idle state can be restored by* ***clearing the RTS timer****.*

3)*Channel can prepare for the next message by setting an* ***Ack Time Out*** *when a message comes during the sending Data feature.*

Phase 3: Send Functions

Send RTS: If (its attempts >= 1), send RTS on a free channel from spectrum sensing with the given parameters (source, Destination, Proposed Channel); otherwise, if no response is received, if multiple RTS are enabled through the rtsAttempts parameter, send another RTS; otherwise, if failed RTS Attempts, inform app layer by sending a nack and re-initialize its attempts parameter to the number of RTS.

Send CTS: Send CTS with the existing parameters (Source, Destination, ProposedChannel) and set isReceiving = true to begin data transfer.

transmit Data: This is a two-case data transmission technique:

Case 1: if (currentDataChannel = 1 or 2 or 3) then set

Display icon.

Case 2: if ackEnabled == true (Only send the next packet after receiving the previous one)

ACK) with 2 steps:

If currentDataChannel! =0, the **first step** is to send a frame.

Step 2: if not, use the suggested Idle function (get Idle)

Send Nack: send this message through an unreliable transmission and reception situation, such as an issue with data lower and ctrl upper.

hardware of a transceiver based on "Software Defined Radio (SDR)" that is interfaced to all available radio frequency spectrum channels and performs all signal processing in software. Instead of many different types of wireless simulation scenarios in which each "MAC protocol" required one or more Network Interface Card modules to be represented as the physical layer.

This feature allows for dynamic changes to implementation parameters without requiring the transmission to be switched to a new NIC module. Another valuable aspect of the proposed scheme is the use of an adjusting approach based on the spread spectrum technique Frequency-hopping spread spectrum (FHSS) as (ten frequency bands) to avoid interference and jamming attacks with dynamically shifting current data channel after detecting another idle channel (proposed channel) with another channel band.

The proposed system simulated in the (Physical layer) and (Data Link layer). Other modules provide assistance for the intended work by enabling layer connections and signaling:

When using the getParentModule feature, it is possible to locate the responsible variable that started transmitting via the cognitive radio node and is known (address) through the Physical Layer. This method can also be used to calculate the number of open channels for users and idle ones. As well, there is a procedure contained in the files (CrystalPhysicalLayer.h and CrPhyPhys).

Appendix

Physical Layer Algorithm

Address, ctrlUpper, data Upper, ssInterface are some of the input/output variables.

Step 1: Use address Tx = 2 and Rx = 2 in a case to identify which address should be used to initiate transmission to another node, which represents the target node.

Step 2: Begin using the handle

Case 1: If Ctrl msg from MAC msg->arrivedOn("ctrlUpper$i") * arrived, then message is true.

On: Boolean method returns true if any vector gate's value matches.

Case 2: If the MAC sends a data message

send it over the data rate spectrum to the des node

msg->arrivedOn("dataUpper$i")

check and castdataMsg *>(msg); dataMsg *recMsg = check and castdataMsg *>(msg);

broadcast(recMsg);

* A check and cast> that accepts other pointers than cObject*. As a matter of compatibility, OMNeT++ 5.0 and later already include this.

Case 3: By employing the spectrum sensing interface msg, data rate Spectrum was provided with sensing data via the Spectrum sensing interface.

Case 4: As incoming data in receiver mode, messages from the outside world are received as incoming data

It is transmitted as follows if the message is an object message: Check and cast (dataMsg *recMsg = dataMsg *) (msg);)

"dataUpper$o" in recMsg;

It's also possible to determine what the ctrl message is before sending it for sensing, by using the ctrl class

the following code: send (copy, "ssInterface$o)

Step 3: broadcast

Send data messages with output array arriving for all interfaces (ports).

for (int x=0; x<gateSize("radio"); x++) {

dataMsg *copy = (dataMsg *) msg->dup ();

send (copy, "radio$o", x);}

// gateSize: The gate vector's size is returned. There are two types of gates: (1) for non-vector gates, and (0) for either no gate or as an alternative, gate names can be.

CrNetworks: It includes a root network definition file (. ned) that is in charge of executing the project and gathers all classes and methods from another directory as supporting packages, which we call from the namespaces folder. General parameters such as sub-modules (address, neighbors, etc.) and full-duplex connections between nodes are also included.

CrNodes: the layer structure and their interconnections, such as signaling and coordination links, numbers, and cognitive engines, are all included. The original default parameters and their data types, gates, the specification for sub-modules, and some of the graphical user interface display features are also included.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية تكنولوجيا المعلومات

قسم شبكات المعلومات

مقترح لتعزيز نظام أمنية شبكات الراديو الأدراكي

الرسالة

مقدمة الى مجلس كلية تكنولوجيا المعلومات جامعة بابل وهي جزء من متطلبات نيل درجة الماجستير في تكنولوجيا المعلومات - شبكات المعلومات

من قبل

دعاء كريم جاسم صالح

أشراف

أ.د. ستار بدر سدخان

هـ 1443

م 2021

الخلاصة

تم تطوير تقنية الراديو المعرفي (CR) للتغلب على ندرة الطيف بسبب التطور السريع للشبكات اللاسلكية. يمكن لكل من المستخدمين المصرح لهم وغير المصرح لهم استخدام الطيف مع هذه التقنية. يتم توزيع الطيف بشكل ديناميكي في شبكات الراديو الإدراكية ، وبالتالي زيادة استخدام الطيف وزيادة الهجمات ، بما في ذلك التنصت. هناك نوعان من هجمات التنصت ، النوع الأول هو الهجمات السلبية ، ولا يقوم المهاجم بأي تغييرات على المعلومات التي تم اعتراضها. يحتاج المهاجم فقط إلى مراقبة الإرسال. والنوع الثاني يشمل الهجوم النشط تعديل الرسالة ويسبب قدرًا هائلاً من الضرر للنظام ويتم تحقيقه من خلال السيطرة المادية على رابط الاتصال لالتقاط وإدخال الإرسال. البيانات المنقولة محمية من هجمات التنصت بطريقتين. الطريقة الأولى لحماية المستخدم الأساسي من التنصت السلبي هي السماح للمستخدمين الثانويين فقط بمعرفة استخدام القنوات الفارغة ؛ ومع ذلك ، يعتبر أي مستخدم خارجي لا يعرف مهاجمًا ، ولا يُسمح له باستخدام القناة الفارغة. الطريقة الثانية تستخدم خوارزمية تشفير فوضوية حيث يتم تشفير الرسائل قبل إرسالها.

تم اقتراح هذه الدراسة لتعزيز أمن شبكات الراديو المعرفية من خلال تنفيذ الطريقة الأولى التي تستخدم بها خوارزمية التشفير الفوضوي لحماية الرسائل من هجوم التنصت النشط لأن الميزة الرئيسية هي أن الإشارة الفوضوية تظهر للمستخدمين غير المصرح لهم كضوضاء ، و الإشارات الفوضوية حساسة للغاية لظروف البداية والطريقة الثانية يمكن أن تحمي البيانات المنقولة من التنصت السلبي من خلال السماح للمستخدمين الثانويين الذين يعرفونهم من خلال عناوين IP الخاصة بهم باستخدام القنوات الفارغة ، ولكن أي مستخدم خارجي هناك ليس لديه عنوان IP يعتبر هجومًا ، ولا يُسمح لهم باستخدام القناة الفارغة. لذا فإن أمن شبكة الراديو المعرفية هو أحد الموضوعات الأكثر تركيزًا وإثارة للاهتمام.