Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon

ENHANCEMENT OF THE COGNITIVE RADIO NETWORK SECURITY BASED ON RSA AND FREQUENCY HOPPING TECHNIQUE

A Thesis

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

AWS AHMED KADHIM

Supervised by

Prof. Dr. Sattar B. Sadkhan

2021 A.D. **1442 A.H**

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

نَرْفَعُ دَرَجَاتٍ مَنْ نَشَاءُ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ

صدق اللَّهُ العظيم

سورة يوسف /الآية 76

Supervisor Certification

I certify that the thesis entitled (**ENHANCEMENT OF THE COGNITIVE RADIO NETWORK SECURITY BASED ON RSA AND FREQUENCY HOPPING TECHNIQUE**) was prepared under my supervision at the department of Information Networks/ College of Information Technology / University of Babylon as partial fulfillment of the requirements of the degree of Master in Information Technology-Information Networks.

Signature:

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

Date: / /2021

The Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled "ENHANCEMENT OF THE COGNITIVE RADIO NETWORK SECURITY BASED ON RSA AND FREQUENCY HOPPING TECHNIQUE" for debate by the examination committee.

Signature:

Prof. Dr. **Saad Talib Hasson Aljebori**

Head of Information Networks Department

Date: / /2021

Dedication

I hereby declare that this Dissertation, submitted to the University of Babylon in partial fulfillment of requirement for the degree of Master of 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 sources are appropriately cited in the references.

Signature:

Name :**Aws Ahmed**

Date: **/ 1 / 2021**

Acknowledgement

In the name of God, Most Gracious, Most Merciful, At first, Praise be to God and thanks to God and the satisfaction of parents and conciliation only from God greatest praise is to **Allah** for His assistance in facing the difficulty that I met in my study, and for always helping me to achieve my aims, also for His great graces and boons all the time.

I would like to express my deepest thanks to my supervisor **Prof. Dr. Sattar B. Sadkhan** for his valuable advice, motivation, guidance, and for so many fruitful discussions throughout the preparation of this thesis.

I would like to extend my respect and deepest gratitude to the College of Information Technology and coordination between the Ministry of Interior and the presidency of the University of Babylon

Sincere appreciation and love go to my family, my father who I wish to be present and my dear mother that whatever I did to her will not reward her they provide me with optimism and pure affection and they give me great hope, encouragement and they have stood with me in every step in this research.

Finally, Sincere thanks and appreciation to all friends, colleagues and loved ones

Abstract

Cognitive Radio (CR) is the technology of used free spectrum band based on the main elements as the primary and secondary users, through the structure can sense the surrounding environment and adapt to the different operating parameters to enhance the communication quality. A flexible and adaptable physical layer implementation is needed to achieve a better enhancement cognitive radio system.

In this thesis, the proposed system based on the most beneficial spread spectrum technique in Cognitive Radio Networks based on the used parameters determined as the Frequency-hopping spread spectrum (FHSS) to attend the Physical layer requirements within Cognitive Radio architecture. The used system based on the Throughput, Data Drop Rate, Detection Time and Delay Time simulation parameters.

Besides, the proposed system simulates Noise-Jamming attack in cognitive radio network Environment. Moreover, the proposed system has been done using OMNET++ simulation tool. So, it simulates the security system with (6 CR or Secondary Users) labeled as military units and (20 Primary Users) placed as a licensed frequency band GSM units.

Simulating Noise-Jamming attack in CRNs environment in all case studies where the used system presents the Noise-Jamming attack effects by decreased Throughput , increased data drop rate, detection Time and delay Time.

The Results of CR Simulation state show that the case study of FHSS is better than compared with the case studies of RSA and RSA-FHSS depending on the simulation parameters as Throughput, Data Drop Rate, Detection Time and delay time.

While the best case study used to mitigate Noise-Jamming attack is the compound system based on the RSA-FHSS case study.

Abstract

Cognitive Radio (CR) is the technology of used free spectrum band based on the main elements as the primary and secondary users, through the structure can sense the surrounding environment and adapt to the different operating parameters to enhance the communication quality. A flexible and adaptable physical layer implementation is needed to achieve a better enhancement cognitive radio system.

In this thesis, the proposed system based on the most beneficial spread spectrum technique in Cognitive Radio Networks based on the used parameters determined as the Frequency-hopping spread spectrum (FHSS) to attend the Physical layer requirements within Cognitive Radio architecture. The used system based on the Throughput, Data Drop Rate, Detection Time and Delay Time simulation parameters.

Besides, the proposed system simulates Noise-Jamming attack in cognitive radio network Environment. Moreover, the proposed system has been done using OMNET++ simulation tool. So, it simulates the security system with (6 CR or Secondary Users) labeled as military units and (20 Primary Users) placed as a licensed frequency band GSM units.

Simulating Noise-Jamming attack in CRNs environment in all case studies where the used system presents the Noise-Jamming attack effects by decreased Throughput , increased data drop rate, detection Time and delay Time.

The Results of CR Simulation state show that the case study of FHSS is better than compared with the case studies of RSA and RSA-FHSS depending on the simulation parameters as Throughput, Data Drop Rate, Detection Time and delay time.

While the best case study used to mitigate Noise-Jamming attack is the compound system based on the RSA-FHSS case study.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Description
ACK	Acknowledgement
AMC	Adaptive modulation/coding
AES	Advanced Encryption Standard
AI	Artificial Intelligence
BSs-APs	Base Station-Access Point
BAN	Body Area Network
CE	Cognitive Engine
CR	Cognitive Radio
CR-WSN	Cognitive Radio - Wireless Sensor Network
CRNOMA	Cognitive Radio Non-Orthogonal Multiple access
CWSN	Cognitive Wireless Sensor Networks
CCSD	Control Channel Saturation DoS Attack
DoS	Denial of Service
DBMUD	Density-Based MU Detection
DFH	Differential frequency hopping
DS	Digital Signature
DS- CDMA	Direct Sequence Code Division Multiple Access
DSSS	Direct Sequence Spread Spectrum
dybit	Dynamic Bit
DFH	Dynamic Frequency Hopping
DSA	Dynamic Spectrum Access
ECC	Elliptic Curve Cryptography
FSS	Fraternization Spectrum Sensing
FB	Frequency band
FH	frequency hopping
FHKE	Frequency Hopping based key Distribution
FHDSA	Frequency Hopping Dynamic Spectrum Access
FHSS	Frequency-hopping spread spectrum
GFSK	Gaussian Frequency-Shift Keying
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HDS	High Data Sensitivity
HMI	Human Machine Interface
ISI	Inter Symbol Interference

LA	Learning Attack
LoS	Line of Sight
LDS	Low Data Sensitivity
MDS	Medium Data Sensitivity
MS	Mobile Station
MC-CDMA	Multicarrier Code Division Multiple Access
MUI	Multiuser Interference
NBI	Narrowband Interference
ND	Network Description
OFA	Objective Function Attack
PLS	physical layer security
PU	Primary User
PUE	Primary User Emulation
PUEA	Primary User Emulation Attack
QoS	Quality of services
RF	Radio Frequency
RC	Rivest Cipher
RSA	Rivest-Shamir-Adleman
RTS-CTS	Request To Send - Clear To Send
SU	Secondary User
SHA	Secure Hash Algorithm
SCN	Selfish Channel Negotiation
SCL	Signaling & Communication Link
SDR	Software Defined Radio
SSDF	spectrum sensing data falsification
TKIP	Temporal Key Integrity Protocol
TTA	Tidal Trust Algorithm
ToA	Time of Arrival
TPC	Transmit Power Control
UWB	Ultra-wideband
UAV	Unmanned Aerial Vehicle
WPA 2	Wi-Fi Protected Access 2
WEP	Wired Equivalent Privacy
WRAN	Wireless regional area network

List of Symbols	
Symbol	**Description**
$\boldsymbol{M^e}$	M(plain-text), e public key index
C	Cipher-text
P	Public Key
q	Private Key

CHAPTER ONE

Introduction

1.1 Introduction

Cognitive Radio (CR) is the technology of used free spectrum band based on the main element as the primary, secondary users, through the structure can sense the surrounding environment and adapt to the different operating parameters to enhance the communication quality. The key term of control the radio frequencies scarcity is using cognitive radio (CR) as a smart and dynamically reconfigurable radio using a dynamic spectrum access paradigm to make better use of the radio spectrum [1].

The radio spectrum is divided into licensed and unlicensed frequency bands. The licensed spectrum used for private users, for example, TV broadcast, Global System for Mobile Communications (GSMs) and so on. The unlicensed spectrum used available for free by anyone, for example, Bluetooth. Cognitive Radio makes use of unused licensed radio frequencies, known as spectrum holes through given time and location via enabling secondary users CR to autonomously access spectrum holes to increase performance. As a matter of fact, secondary users should take into consideration not to harmfully interfere with the primary users' licensed spectrum [2].

The Cognitive radio works in the radio environment, when there are Radio Frequency motives CR sense to recognizing unused spectrum to find spectrum holes and release the channel when a licensed user (Primary User) is discovered based on spectrum mobility characteristic, then decide with decision rule depends on specific parameters to make decision making, which is selected the idle channel then spectrum sharing provides access to the chosen channel with other users by spectrum scheduling these are operations known as a cognitive cycle [3].

The Figure 1.1 , shows operations which were closely related to cognitive radio characteristics through the cognitive radio operation cycle [4].

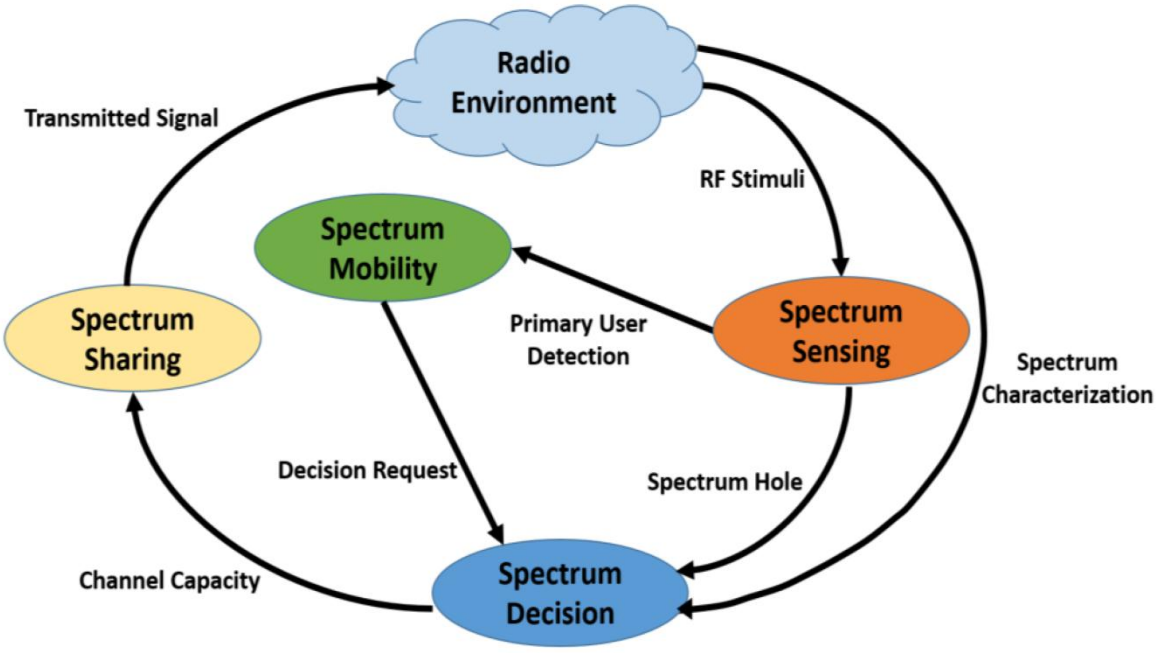
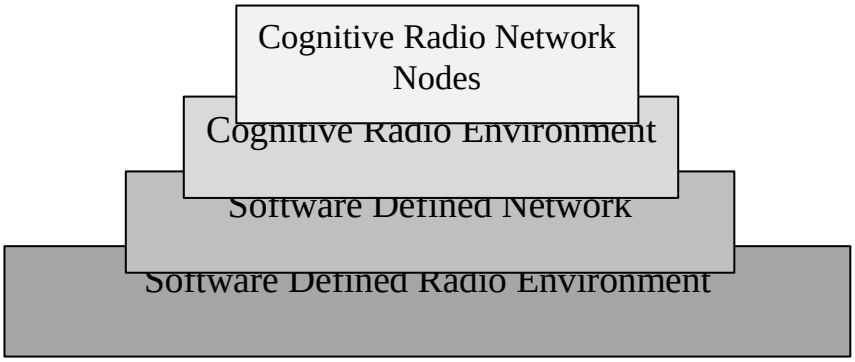


Figure 1.1: Cognitive Radio Operations Cycle.

The core structure of Cognitive Radio based on the concept of the Software Defined Radio (SDR) technology, where SDR is examined as the typical platform approach for CRs applications. This mixing analyzed the most suitable solution for many types of wireless problems, for instance, spectrum underutilization approach, geographical localization and so on.

The SDR regularly has a particular interface called Human Machine Interface (HMI). It is a sensor of the environment that enables the user to input management directions for the Cognitive Radio application. Besides, when there is a condition for user identification or authentication purpose, So it used a biometric sensor with it for this situation, Software Defined Radio (SDR) and Artificial Intelligence (AI) technology provides the facilitates for the Cognitive Radio (CR) [5].

The Figure 1.2, shows the relation between the cognitive radio network and Software Defined Radio, and SDR considered the optimal framework to build the cognitive radio network [6].



1.2 Literatures Review

There are many proposed enhancement system for Cognitive Radio Network applications for example within the literature review below from the past to the latest directions:

In (Qusay et al., 2007) the authors achieved trusty and security communications for new battlefield purposes, which becomes a confrontation task nowadays and the focus of researchers through the security considered the central factor in the first place and then bandwidth. Usually, ideal CRN in the military environment is distributed, which enables CR military units to transmit over any radio spectrum band while at the same time control on the network without based on the central unit [7].

In (Wendong et al., 2007) the authors explained how to implement the Dynamic Frequency Hopping (DFH)-Wireless regional area network (WRAN) data transmission, meanwhile assured reliable spectrum sensing and efficient channel mode in parallel system environments [8].

Suggesting a scheme based on the frequency hopping spread spectrum techniques in (Xiaohua et al., 2009) the authors. which operates reliably without any a priori handshaking assuming. The used system based on every cognitive radio separately identifies white spaces and then chooses one of them to send or receive signals according to a pre-defined pattern of the frequency hopping, also deals with large detection errors based on the accuracy of the spectrum sensing [9].

In (Zhuo et al., 2009) the authors implemented the cognitive radio network in an efficient FH technique for an enhanced data rate of High-Frequency communication system knows as Differential frequency hopping (DFH). The proposed network scheme called a CogDFH network. The simulation network produced against the mode of interference temperature, IC-colorings and IC-indices of graphs, the results show the cognitive radio improved with the low interference and high robustness [10].

In (Rajani et al., 2011) the author introduced a specific framework controlling equivalent to the conditions of heterogeneous sensor networks environment to deal with the current security threats and the new one. Through, the framework used as a cognitive security framework, which included the measurement of the affecting single operation on the channel or through distributed Denial of Service (DoS) attacks and predicts a new one supporting both collaborative and non-collaborative sensors nodes, to grant reliable and secure system [11].

In (James et al., 2011) the author discussed the performance of the various security methods and how they effected on the cognitive radio security for instance (Symmetric-key Algorithm: RC5 [block], Asymmetric Key Algorithms: Elliptic Curve Cryptography [ECC]), and the main focus solved current security threats and the new one within a Heterogeneous Communication Network [12].

In (Olga et al., 2012) the authors performed a particular qualitative analysis for current security threats and against new potential threats to evaluate these security threats impact within the performance of the CRNs, besides offered the several methods to deal with a general attack such as the Primary User Emulation (PUE) attack and the concept of new cross-layer attack [13].

In (Sazia et al., 2013) the authors suggested a novel approach for a conjoint trust assessment based on the trust evaluation of the Secondary user

requests, before capturing the ideal Primary User channel. So, the used system enhanced the security effects of Cognitive Radio Networks communication by deals with the problems of the security threats occurring from the untrusted behavior of the malicious entities, faultless and selfish nodes, besides, it ensures the security of the spectrum sharing characteristic in Cognitive Radio Network [14].

In (Mahmoud et al., 2014) the author presented the survey of the main challenges, security attacks and the main mitigation methods in Cognitive Radio Networks(CRNs). The attacks displayed based on the protocol-layer operating attack [15].

In (Adarsh et al., 2014) the authors described the scheme of a soft-real time Cognitive Radio MAC, which contains in various secondary users, within a spread spectrum frequency hopping (FH) as a primary situation. Besides the main job of the proposed MAC scheme of spectrum sensing, which is dynamically allocating the free frequency bands to various Cognitive Radio users depending on the requirements of the Quality of service. Also, the used system detects the primary user hop [16].

In (Qiben et al., 2014) the authors performed a security scheme to minimize the effecting of attacks within wire/wireless of CRNs by using machine learning method using (a systematic passive monitoring framework, SpecMonitor) to discover the behaviors of malicious nodes [17].

In (Helen et al., 2014) the authors explained the definition of the relationship between military applications and the performance of the cognitive radio network role to deal with the different security problems and the effectiveness of the used the Dynamic Spectrum Access(DSA) technology advantages for Radio Frequency, besides, intrusion restriction, additionally the used system illustrated the opportunity of developing a CRNs system to deal with context percipient takes into

consideration the preference of the incoming transactions messages among the cognitive radio nodes in tactical circumstances [18].

In (Bhagavathy et al., 2014) the authors addressed the opportunity of implementation of aggregating the Symmetric/ Asymmetric encryption algorithms for instance (Rivest-Shamir-Adleman, Elliptic, Secure Hash Algorithm, Digital Signature)to secure CRNs environment, in addition to that the used spread spectrum modulation schemes for decreasing various layered attack types, a further implementation state of the Kerberos algorithm for secure session verification by restricted the used shared keys for preventing the intruder from generating the session key to get access for highly secure communication [19].

In (Mohandass et al., 2014) the authors investigated the study of various types of modulation schemes as multi-carrier types and spread spectrum methods such as Direct Sequence Code Division Multiple Access (DS- CDMA), Multicarrier Code Division Multiple Access (MC-CDMA). So, the used system implemented different types of improvement schemes to decrease interference like Inter Symbol Interference (ISI) , Multiuser Interference (MUI) and robustness against Narrowband Interference (NBI) [20].

In (Anssi et al., 2015) the author converged the security of battlefield applications as the main applications of crucial Cognitive Radio Networks via the used system produces a specific cyber-security structure, where the suggested system leading to discover the vulnerabilities and minimize security weaknesses through improving the security requirements of the main tactical networks like military networks [21].

In (Kresimir et al., 2015) the authors displayed the effecting of Cognitive Radio technology on critical military applications, which it describes as the

important CRNs applications, moreover, the used system deals with security threats like jamming and anti-jamming threats based on a game-theoretical framework, and how they associated with Radio Frequency (RF) within specific architecture testbed like a Software Defined Radio/Cognitive Radio. So, the novel algorithms (Spectrum Intelligence for Interference Mitigation algorithm) improvement and examination achieved within a real-time monitoring state [22].

In (Navpreet et al., 2016) the authors used a way for Spread Spectrum techniques analyzing within Cognitive Radio Networks(CRNs). The investigated work based on the two spread spectrum methods as a particular Direct Sequence Spread Spectrum (DSSS) and Frequency-hopping spread spectrum (FHSS) reviewed concerning with the Physical layer of the cognitive radio network. Moreover, doing the differences between these spread spectrum techniques using MATLAB, Where, the used simulation illustrating FHSS operates better than DSSS implemented in CRNs based on the parameters such as Throughput, Data Drop Rate, and Detection Time [23].

While in (Chao et al., 2016) the authors suggested a specific cryptography scheme based on the Frequency Hopping Dynamic Spectrum Access (DSA) as (FH-DSA), through, presenting the pattern of Dynamic Bit(dybit), which describes the nature of the binary value and the DSA approach. The proposed system takes into consideration the difficulty of the dybit state. The particular mechanisms used as a Frequency Hopping based key Distribution (FH-KE) to build security communication, Also, restricting the collisions of the data packet through the group FH-KE (GKE), a confidentiality-oriented DSA scheme [24].

In (Yongcheng et al., 2016) the authors introduced a hybrid Primary User Emulation Attack (PUEA) detection method, based on the pattern measurement of the spectrum expanding which is based on the time rate changing of the mobile radio channel known as Doppler spread. The performance of normal

behavior mobile SU and PU have Doppler spread, which may be different compared with the malicious behavior among the SUs and the Primary User Emulator (PUE) attack because of different relative speeds. However, maybe affected the relative location among the SUs and the PUE [25].

In (Hongxing et al., 2016) the authors suggested a particular detection algorithm for Wide-band frequency known as Density-Based MU Detection (DBMUD) specifically. So, The used system decreases the security threats from the effectiveness of the Spectrum Sensing Data Falsification (SSDF) attack in Cognitive Radio Network [26].

In (Ameer et al., 2017) the authors suggested the keywords sensitivity identification method of military applications in secure Cognitive Radio Networks (CRNs) environments, Where the used system based on high data sensitivity content recognition to match text messages into High Data Sensitivity(HDS) for high priority words, Medium Data Sensitivity(MDS) for less priority message content and Low Data Sensitivity(LDS) for lower message exchanges from the sender to the target node. The cryptography system based on the Advanced Encryption Standard/Wi-Fi Protected Access 2, (AES/WPA2), Frequency-hopping spread spectrum (FHSS) equivalent to the HDS. The Rivest Shamir Adleman (RSA) applied to MDS and Rivest Cipher (RC4) to LDS for all message content transferred among CR nodes [27].

In (Fatima et al., 2017) the author discussed the main comparisons among existing spectrum sensing techniques used for Cognitive Radio Networks(CRNs).The comparisons parameters such as "energy, autocorrelation, Euclidian distance, wavelet, and matched filter based sensing". Also, the work presents the problem of spectrum management, the cognitive radio cycle and the solution with compressive sensing [28].

In (Elanagai et al., 2017) the authors proposed a novel model based on the protocol of Hence Fraternization Spectrum Sensing (FSS) to mitigate network security attacks, enhancing the power consumption and minimize system delay, It applied with cooperative sensing process and calculating trust values for each secondary users subsequently, besides, it enhanced the network security based Data Televising [29].

In (Nasrin et al., 2018) the authors explained Secondary Users can arrive the spectrum permanently in case not harmful Primary Users. Moreover, SU doesn't require to leave the frequency spectrum through PUs return. The used method very helpful and effective because it enhanced the CR performance in various wireless networks and IoTs environments, Where it was based on a method for calculating the variables of the distance between the nodes and adopting a method for Line of Sight (LoS) and Time of Arrival (ToA) to calculate the distance between the sender and the receiver nodes[30].

In (Sarala et al., 2019) the authors defined a cross-layer approach as a strategy for identifying the PUEA within a CRN. Besides several attacks explained and how to disclose PUEA based on the authentication schemes. The used system shows the physical layer authentication scheme works more high-speed authentication process except for the low accuracy detection process. While authentication protocol cryptography works slower authentication process besides powerful high accuracy detection [31].

In (Zhongwu et al., 2019) the authors examined the Physical Layer Security (PLS) within CRN as the network approach of Non-Orthogonal Multiple access (CRNOMA) including various PUs and SUs. The used system based on NOMA strategy to handle the user interferences and ensure the PUs with Quality of Services (QoS) feature. So, PUs and SUs primary implements with including channel gains [32].

Table 1.1, illustrates the aims of previous researchers trends and what the simulation tools which are used to achieved the works.

Table 1.1: The aim of Researchers and The used Simulation Tools.

Frefe.No Year	Aims of the work / Year	Simulation tool	Still open problem	Solved problem
[7]. 2007	Achieving trusty and safety communications in new battlefields applications.	C++ , Java	self-management through system mobility	Making battlefields applications secure
[8]. 2007	Implementing reliable spectrum sensing and efficient channel usage in parallel for CRN system.	Optimization Tool	Analysis the used protocols especially for policies driving communication	Reliability in spectrum sensing
[9]. 2009	Suggesting a scheme of the FHSS techniques. which operates reliably without any a priori handshaking assuming.	Monte-Carlo	SUs transmitter coordination	Detecting errors based on the accuracy of the spectrum sensing
[10]. 2009	Implementing CR in an efficient FH technique.	Monte-Carlo	Interference from multi-user case	Enhancing data rate of High-Frequency communication system
[11]. 2011	Determining existing and new security threats in a Heterogeneous Communication Network effected on the cognitive radio security.	NS2	Computation power management	Solving security threats in Heterogeneous Networks
[12]. 2011	Solving existing threats in CRNs.	Monte Carlo and MATLAB	Predict the effectiveness of the new attacks	Providing secure and reliable CR system
[13]. 2012	Measuring how can attacks impact CRNs performance.	MATLAB and NS-2	PUE of TV broadcast bands, detecting PUE attack in mobility case.	Detecting Primary User Emulation (PUE) and a new cross-layer attack
[14]. 2013	Solving the security problems occurring through untrusted entities' behavior, like malicious, faultless and selfish nodes, besides.	OMNET ++	Verification of trust for CRN ubiquitous computing	Solving the security problems and secure spectrum sharing in CRNs
[15]. 2014	Making a survey of supporting methods used	/	Presented the used methods	Interference problems

	for security CRNs.			
[16]. 2014	Describing the scheme of a soft-real time Cognitive Radio MAC, within a spread spectrum frequency hopping (FH).	GNU Radio, Universal Software Radio Peripheral (USRP)	Distributed SU network, Design control channel	Detecting the primary user hop
[17]. 2014	Decreasing attacks and protect the communication in core wire / wireless CRNs networks.	MATLAB	Reducing abnormal of SUs	Secure the core wire / wireless CRNs networks.
[18]. 2014	Explaining the relationship between military applications and the role of the cognitive radio network.	High Fidelity HiFi	Computation power resources	Determining several security issues
[19]. 2014	Explaining the opportunity of secure CR by using the combinations of encryption algorithms.	Not determined	Centralized Authority	Mitigating the different type of CR layered attack.
[20]. 2014	Implementing the improvement models to mitigate interferences from Inter Symbol Interference (ISI), multiuser interference (MUI) and robustness against Narrowband Interference (NBI).	MATLAB	Optimal Resource Allocation	Mitigating interferences
[21]. 20015	Detecting the weaknesses and mitigating security vulnerabilities.	Software-programmable Approach	Evaluating the security of tactical military networks	Enhancing the security of tactical military networks within CRNs environment
[22]. 2015	Investigating the impact of CR technology on military applications.	OMNEST , OPNET, NS-3 and QUALNET	examination MANET within real environments	Examining intelligent jamming and anti-jamming between the CR nodes
[23]. 2016	Analyzing CR based on DSSS and FHSS with parameters.	MATLAB	Sensing channel of Full –Duplex	Analyzing CR Throughput, Data Drop Rate, and Detection Time.
[24]. 2016	Building a specific cryptography FH-DSA and FH-KE.	Not determined	Confidentiality of oriented DSAs	Creating security communication, Also, restricting the collisions

				of the data packet
[25]. 2016	Investigating (PUEA) detection problem in mobile secondary user (SU).	Monte Carlo	PUEA detection in PUs	Detecting PUEA in CRNs
[26]. 2016	Protecting against a Spectrum Sensing Data Falsification (SSDF) attack.	MATLAB	Computation power	Solving CRNs against Spectrum Sensing Data Falsification (SSDF) attack
[27]. 2017	Implementing the keywords sensitivity identification method of military applications in secure Cognitive Radio Networks (CRNs) environments.	OMNET++	Encryption state	Enhancing throughput and the level of security
[28]. 2017	Discussing the main comparisons among existing spectrum sensing techniques used for CRNs.	Not determined	/	Spectrum sensing based on parameters energy, autocorrelation, Euclidian distance, wavelet
[29]. 2017	Mitigating network attacks.	NS2	Investigating new attacks	Improving the power conception and minimize system delay
[30]. 2018	Explaining Secondary Users can arrive at the spectrum permanently in case not harmful Primary Users and enhancing the CR performance in various wireless networks and IoT environments.	Not determined	Spectrum sharing of CRNs nodes in IoT applications	Spectrum sensing in wireless and IoT networks
[31]. 2019	Defining a cross-layer approach as a strategy.	Not determined	authentication approach of new cross layer attacks	identifying the PUEA within a CRN
[32]. 2019	Examining the physical layer security (PLS) within CRN as the network approach of non-orthogonal multiple access (CRNOMA) including various PUs and SUs.	Monte Carlo	PLS performance in overlay CR-NOMA networks	handle the user interferences and ensure the PUs with quality of services (QoS) feature

1.3 The Aim of the Thesis

The thesis is developed a Cryptosystem to enhance the security of Cognitive Radio Networks by implementing:

1- Public-key encryption methods called Rivest, Shamir, and Adelman (RSA)
2- Adapting method based on Spread-spectrum techniques like a Frequency hopping spread spectrum (FHSS).
3- Enhancing CR with the main simulation parameters used such as the Throughput, Data Drop Rate, and Detection Time simulation parameters.
4- Overall these modules to protect the communication from malicious users and improve the security of military application based on cognitive radio to accomplish a reliable and flexible protection system.

1.4 Thesis Outline

Furthermore, this thesis contains four chapters in addition to chapter one:

Chapter Two: It presents the cognitive radio Network (characteristic, Network architecture, Advantages and challenges of CRNs, Common Application areas of cognitive radio networks,). Also, it shows security issues like security requirements, security attacks in CRN layers and security challenges. Furthermore, a still open problem and common simulation tools explained in this chapter.

Chapter Three: It presents the proposed system and illustrates the practical stages of the system and explains the proposed algorithms system

Chapter Four: It describes the results and evaluates the used system.

Chapter Five: It presents the results conclusion. Also, it described the future works suggestions.

CHAPTER TWO

Theoretical Background for Information Security System in Cognitive Radio Networks

2.1 Introduction

Cognitive radio networks are one of the most important techniques that have been found to solve radio spectrum problems. In general, fixed spectrum assignment policies for wireless applications significantly waste spectrum resources that are considered to be valuable as a result, and which will be spectrum scarcity. Cognitive radio technology, invented by Mitola, is based on an efficient way to utilize available unused channels through the wireless spectrum range by automatic detection method based on the concept of Dynamic Spectrum Access (DSA) [33].

The cognitive radio system is divided depending on, how it enables secondary users handling the Licensed Band into three main paradigms:

The first type known as the Underlay Paradigm. In this type, The Secondary User (SU) transmits at the same time with the primary user (PU), As long as, the interference generated by SU is below a particular threshold. It's common using in the licensed spectrum for instance, Ultra-wideband (UWB) communications. Besides, it's also be used in the field of the unlicensed spectrum bands to produce different user services.

While the second type called the Overlay Paradigm, so, The transmitter of SU identifies the channels furthermore, the messages with codebooks of the PU. It transmitted simultaneously with PU, As long as, the interference is decreased by some collaboration, For example, via the concept of relaying. In the Licensed Bands case, SU would be allowed to work within the Frequency band (FB), and in this case, it can sharing with PU, the Cognitive User would not interfere with PU, it gives PU gaining characteristic for their FB, and communications system employing this knowledge in many ways to either cancel or mitigate the interference seen at the SU and PU. Similarly, while in the second case the

cognitive users in unlicensed bands improve using the channel with higher spectral performance.

The third type is an Interweave Paradigm, in this paradigm the SU operates in an Opportunistic Transmission method to gain access to a specific state called Spectrum Holes or white spaces licensed spectrum band which is used to data transmission, for example, through using TV White Spaces [34]. An important point to clarify that the used system based on the third paradigm (Interweave Paradigm). In Figure 2.1, shows three main paradigms in cognitive radio.

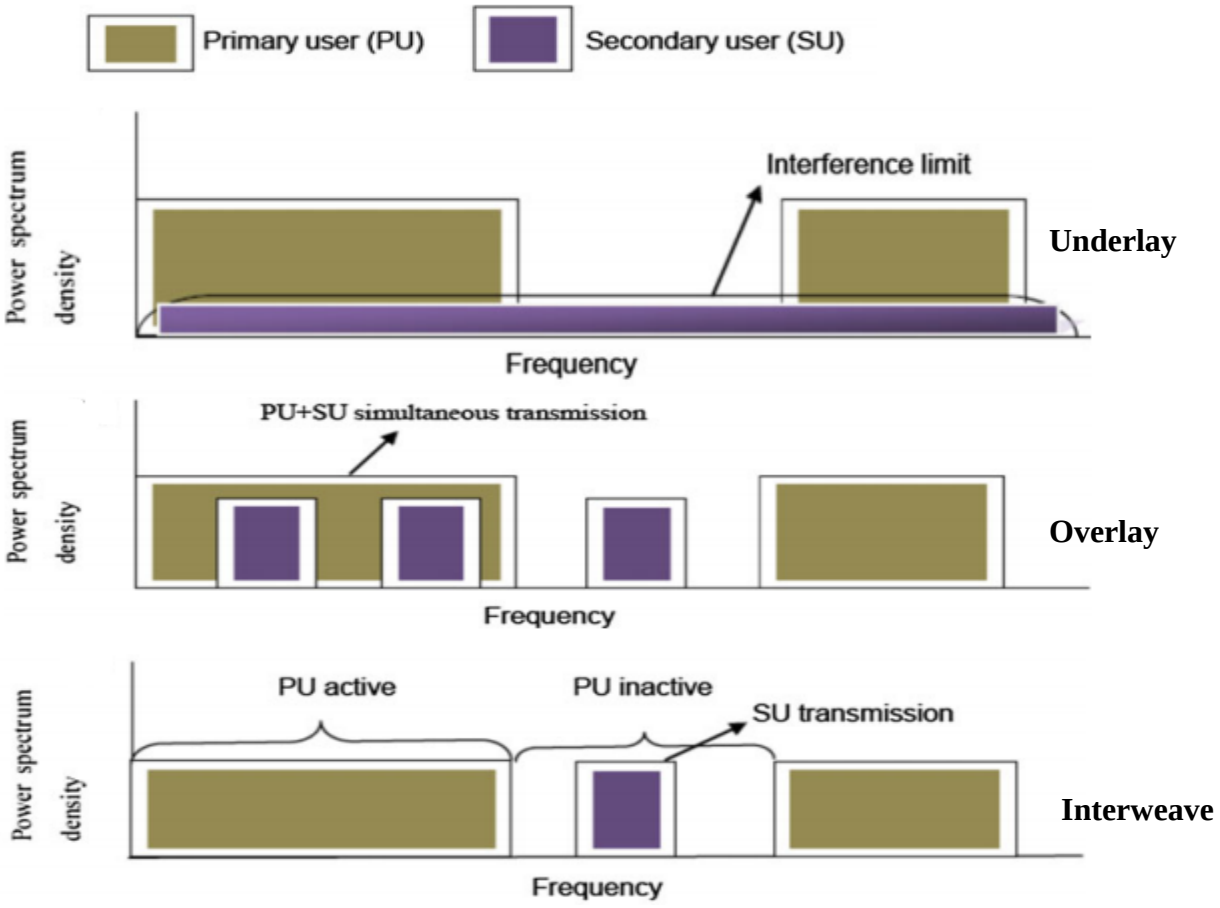


Figure 2.1: cognitive radio paradigms.[34]

2.2 Cognitive Radio Network

The cognitive radio node is classified based on cognitive functionality within the cognitive cycle. Where it is sensing to a collection of environmental parameters, it has the capability to the self-organized setting as well as accommodates to reconfigurable itself in a very flexible and transparent way. So Cognitive capability can be summarized as follows [35]:

- **Spectrum Sensing** : It explained by the ability of the Cognitive Radio Node to discover the Spectrum Holes in the Frequency Band, taking into consideration without interfering with the primary user [36].
- **Location Identification**: It defines as the ability of the cognitive radio elements to identify the location of itself as well as the location of the other transmitter nodes inside the network. There are different ways and forms of how to collect the information of the location, including it is a manual way or it depends on another external way with another extended geographical location system [37].
- **Discovering the Network/System**: Generally, the cognitive node can perform the best way to communicate and share network characteristics, So to do that it must discover the available networks within the coverage area. Consequently, and then it can get access to the network by directed one hop-multi hop communication nodes [38].
- **Discovering the Services**: It stands to reason, when the network discovered and CR nodes connected into the network, it's reasonable to obtain the network services, so this characteristic is associated with network discovery ability and then the opportunity of finding the suitable service satisfied to the node specifications [38].

- **Cognitive Capabilities** : It described as the ability of the CR node to reconfigure the own system. So, the characteristics are summarized in the following points:
- **Frequency Agility**: It represents the ability of the CR node to modify dynamically the parameters of frequency procedures in a to choose the best frequency channel depending on the sensitivity of signal transmitters [39].
- **Adaptive modulation/coding (AMC)**: It evolved as a concept for channel capacity within fading Channels, by it means the ability of the CR node to qualify the transmitter properties to effect on the improving spectrum access with the optimal performance by determining the most suitable modulation type [40].
- **Transmit Power Control (TPC)**: It provides the ability to devices to dynamically adapt the transmission power levels in the data transmission process based on the selective mechanism way to lower efficient power level [41].
- **Dynamic System-Network Access** : It often used within the Heterogeneous Wireless Networks situation, So, the CR nodes reconfigure their own system to operate different protocols which needed to obtain the various Systems-Networks communications [42].

In addition to the above-mentioned characteristics that make the cognitive radio network possess the ability to self-reconfigure itself, which enables it to operate with various types of devices and systems requirements as a smartness technology, for example, it can be based on the Spectrum-Radio Resource management, Mobility with Connection Management and Security Management to provide maximum network performance. [35]

2.3 Cognitive Radio Network: Benefits, Disadvantages and challenges

One of the most important characteristics that made cognitive radio network receive this great attention is the ability to increase the availability of spectrum in wireless networks, and get the scarcity of the radio spectrum. It can sense with the parameters for each environment based on the requirements of the application .Besides, it used for its purpose as it is used in applications of different types of data including audio, image, text, and video streaming. It is worth noting that the used system depends on the text for the data type transmission [43].

One of the widely used features of the cognitive radio network is the multidisciplinary feature. Due to the heterogeneity of its uses, as its benefits evolve in the medical, military, agricultural, and industrial fields, and the vehicle sensor network. The benefits of various applications can be summarized with the following points:

1. Changing spectrum access dynamically.
2. CRNs are self-organizing.
3. Real-time spectrum performance.
4. Increasing spectrum utilization.
5. Enhancing the adaptability of emerging systems.
6. Improving channel capacity within multipath poor environments.
7. Decreasing the cost of the radios spectrum.
8. Mitigating jamming from interference systems.
9. Enhancing SDR techniques based on intelligent algorithms as a Cognitive Engine (CE) [44].

Disadvantages of Cognitive Radio Networks

CRNs have disadvantages summarized with these topics :

1. Sensing techniques require high-speed changeability by switching the sensing channel, which may cause the channel not to be available for communication, as it affects the decision-making in the future step of the optimal channel proposal [44].
2. Prior information considered difficult to get in especially in tactical environments based on matching filtering characteristics of the primary user in operations [45].
3. The nature of wireless medium which is CRNs based on, So, the interference of channel is high mainly for information produced from system resources has high sensitivity [46].

Challenges of Cognitive Radio Networks

Cognitive radio networks have challenges within different applications, and that can be summarized as shown [47]:

1. CRNs routing life-time [48].
2. The problem in collaborative spectrum sensing as the hidden terminal[49].
3. Increased complexity of spectrum sharing algorithm management [50].
4. Difficulties within machine learning information to build knowledge of cognitive radio algorithms[51].
5. Challenges within Disclosure a wideband spectrum sensitivity [52].
6. Cognitive Radio - Wireless Sensor Network (CR-WSN) has hardware challenges as system requirements (storage specifications, power, topology exchanges, and Scalability) which they effected on the WSNs lifetime. Besides, WSNs have challenges within the management of Fault Tolerance, requirements of Quality of Service (QoS) and Security [47].

2.4 Cognitive Radio Networks Architecture

The importance of the cognitive radio network architecture revolves around the nature of the network components and to achieve the main goal of the cognitive radio network architecture by improving the network performance from the user's point of view to provide services anytime and anywhere.

Where this architecture consists of the basic components of CRNs categorized into Mobile Station (MS), Base Station-Access Point (BSs-APs) and Backbone-Core networks. They are the essential parts (MS, BSs-Aps and Backbone-Core) of the three architectures of CRNs: Infrastructure, Ad-hoc and Mesh Architectures [53].

2.4.1 Infrastructure Architecture

This type depends on the basic architecture of the components of the network from infrastructures as backbone base links, interconnect devices such as access points, base stations, communication channels, and cognitive radio network nodes, as well as interfaces that connect the components together.

The Figure 2.2, shows the infrastructure architecture and how network elements connected with each other [54].

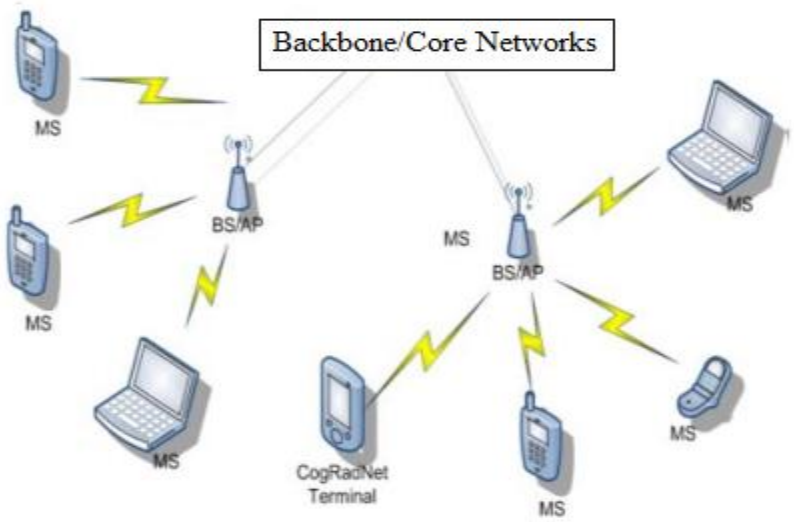


Figure 2.2: Infrastructure Architecture of CRNs.[54]

2.4.2 Ad-hoc Architecture

This architecture is considered as one of the important architectures as it is directly established on-demand among the nodes that wish to communicate and transmit data using radio frequency through the air without the need to rely on the infrastructure provided by the network. For example, by using WiFi, Bluetooth with spectrum holes in spectrum radio. The Figure 2.3, shows the concept of Ad-hoc networks within the Cognitive radio environment [55].

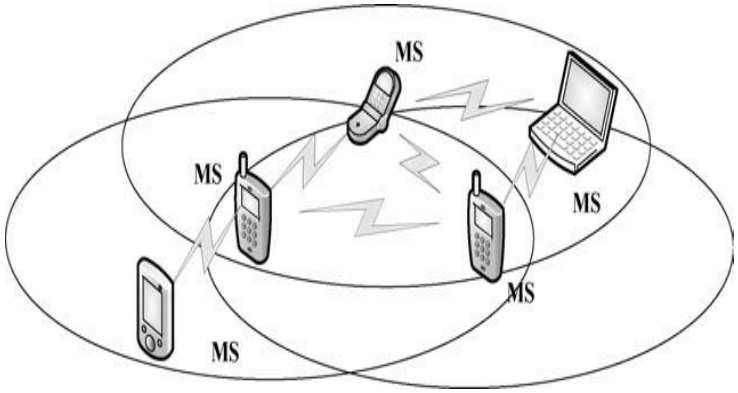


Figure 2.3: The Ad-hoc CRN Architecture.[55]

2.4.3 Mesh Architecture

This architecture is considered as a combination of the two previous types, as it depends within data communication and transmission on infrastructure architecture as well as on-demand Ad-hoc architecture, where it is possible to see the CR mobile station linked to the access points or gateway through the core backbone side within the infrastructure as well as through the CR node with another CR node directly [56].

This architecture allows improving the performance of the network to the optimal level in the cognitive radio environment, as it is based on the benefits provided by the first and second architectural and gets rid of the restrictions and challenges that face both of the two previous architectures.The Figure 2.4 shows the arcitucture of mesh cognitive radio network [57].

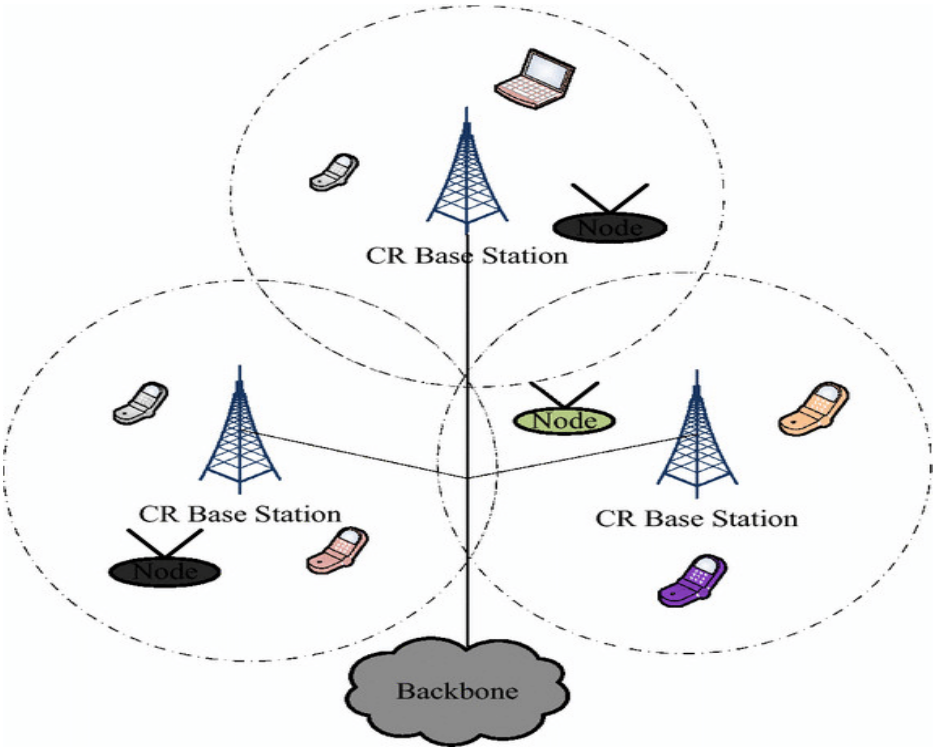


Figure 2.4: Architecture of a CR-mesh network[57].

2.5 Cognitive Radio Networks Applications

Cognitive radio networks used in many applications in the various necessary and important fields of human life, for example, health, agricultural, industrial, commercial and military applications, etc. It performs an important role in wireless consulting applications within the human body as well as accuracy agriculture, remote measurement and follow-up of roads, traffic, the operation of complex systems and services Logistics, as explained in the most important applications of cognitive radio networks in the following parts [58].

2.5.1 Leased Networks

In this type of application, part of the spectrum leased band from the license element (primary user) is used by the secondary cognitive radio node by leasing a portion of the bandwidth in exchange for interest due to the main provider represented by the main nodes. It helps to improve the overall

performance of the network and increase cooperation between the nodes in bandwidth sharing. The Figure 2.5, shows the idea of the leased network [59].

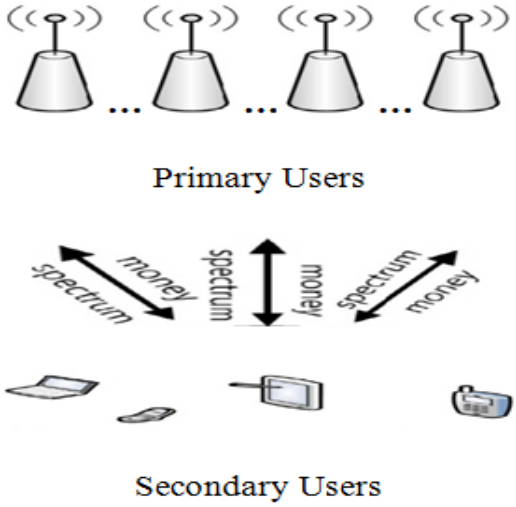


Figure 2.5: Leased Network concept[59].

2.5.2 Emergency Network

The field of wireless communication systems achieves in emergency and rescue networks where it requires the availability of service throughout which requires the services available all day due to disasters natural and human accidents. The role of cognitive radio networks is important in providing services for ambulances, police side and rescue cars by providing a large frequency bandwidth, coverage lost networks areas and isolated networks as a result of natural disasters that caused communication network infrastructure failed [60].

Where the Figure 2.6 shows how to take benefit of cognitive radio networks in relief situations as a result of natural disasters such as earthquakes, floods and other situations that cause the network to be separated and its related agencies [61].

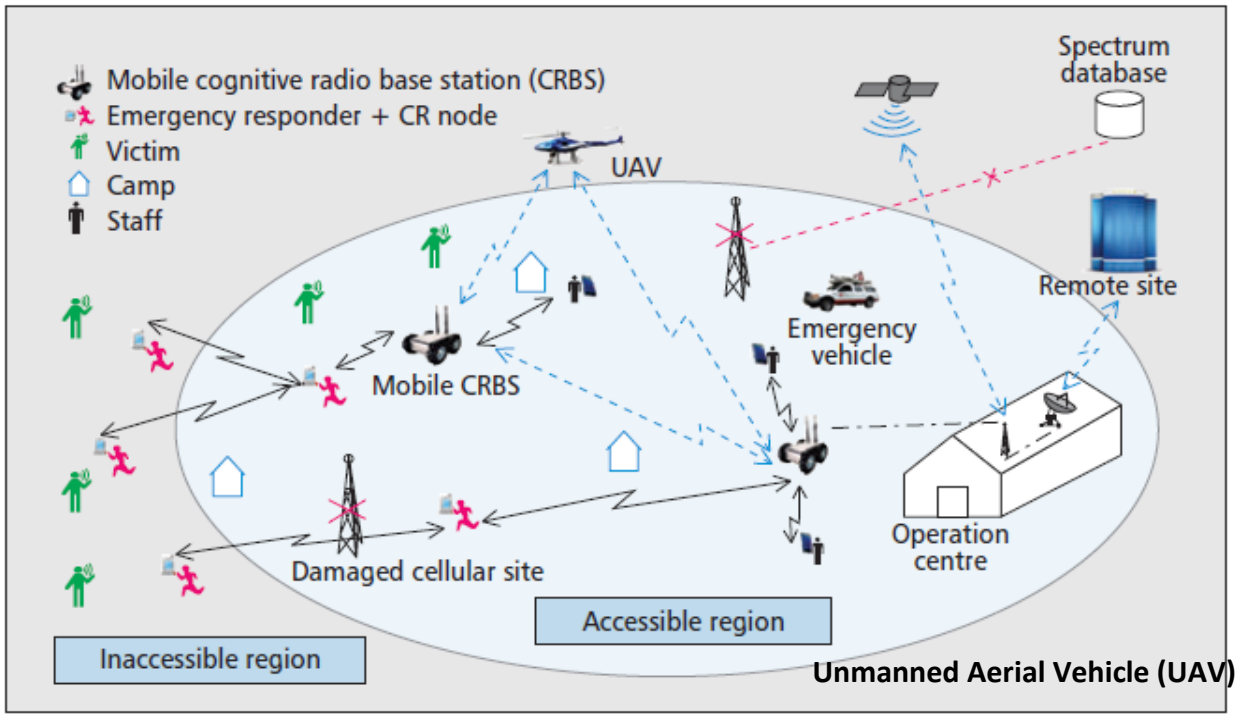


Figure 2.6: Emergency Network Scenario[61].

2.5.3 Military Applications

Military applications are considered the most challenging at nowadays, as they require a high degree of security and privacy to provide security in various areas among the military units of different military classifications, as well as between army soldiers and carriers vehicles, and aircraft, which require the requirement of quality of service (QoS), high degradation scope and rapid response.

The Figure 2.7, shows how to use the cognitive radio network in the military application of various military classes among land and air units and the adoption of the LAN as well as wireless networks [62].

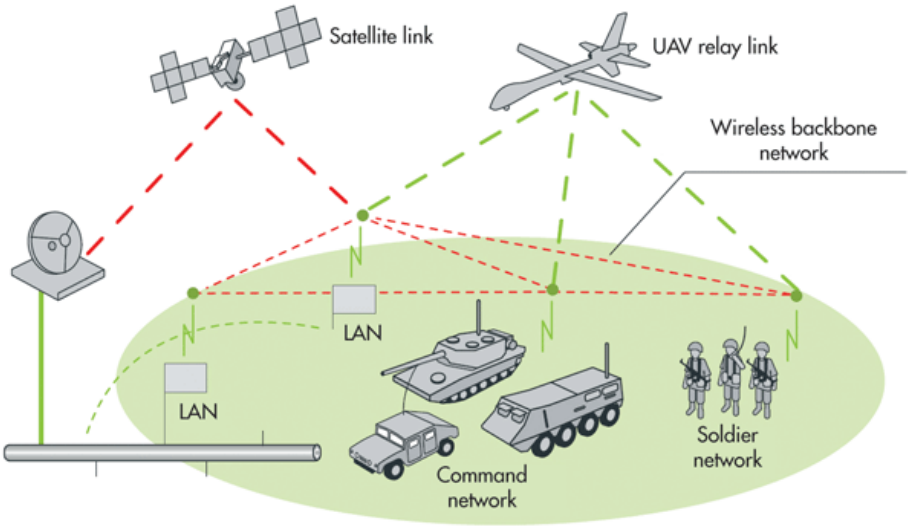


Figure 2.7: CR Military Application [62].

Besides, The Figure 2.8 shows the military application of CRNs to achieve communication between linked nodes in a particular network, for example, combat network radio with the central nodes and how to secure voice communication.

It is well known that the dynamic nature of the Dynamic Spectrum Access (DSA) bandwidth on which cognitive radio networks are based makes the tracking and jamming of communication more difficult. As the cognitive radio network provides the special requirements for securing a radio network on a wide frequency band that can work in a large military environment [62].

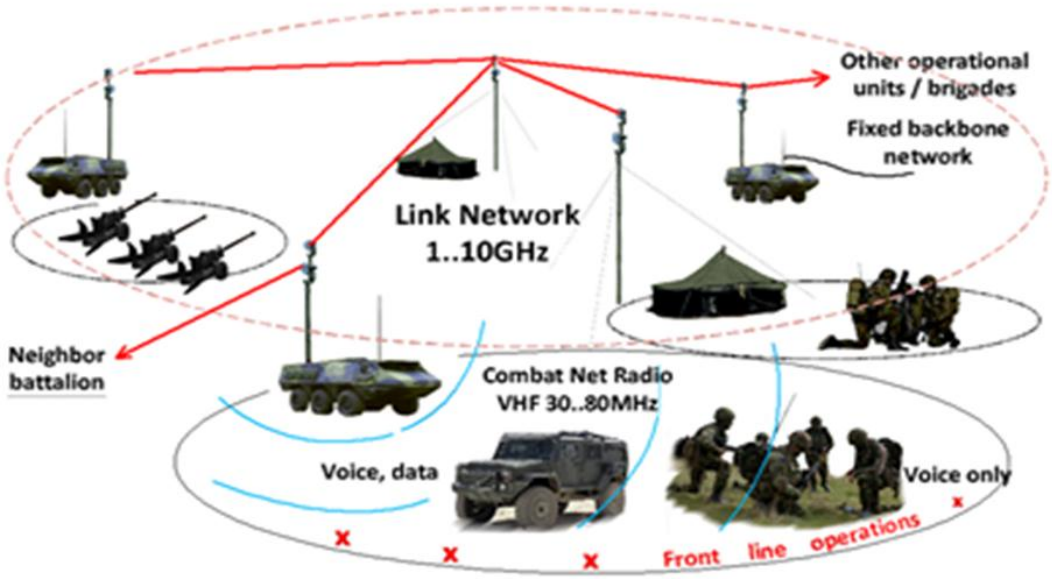


Figure 2.8: CR Battlefield Application [62].

2.5.4 Health Care Implementations

The cognitive radio network also plays an important role in health care systems or medical fields where various types of sensors are used inside and outside the human body where patients are dealt with and monitor data acquired at a distance using these sensors.

As is known about the medical data related to human life is very crucial and sensitive, where using traditional WSNs, they are restricted to remote control, especially in congested overloading situations. So, using cognitive radio networks in this aspect has achieved quality of service (QoS)at a high level as used in the case of a Body Area Network (BAN), which is illustrated in Figure 2.9, [63].

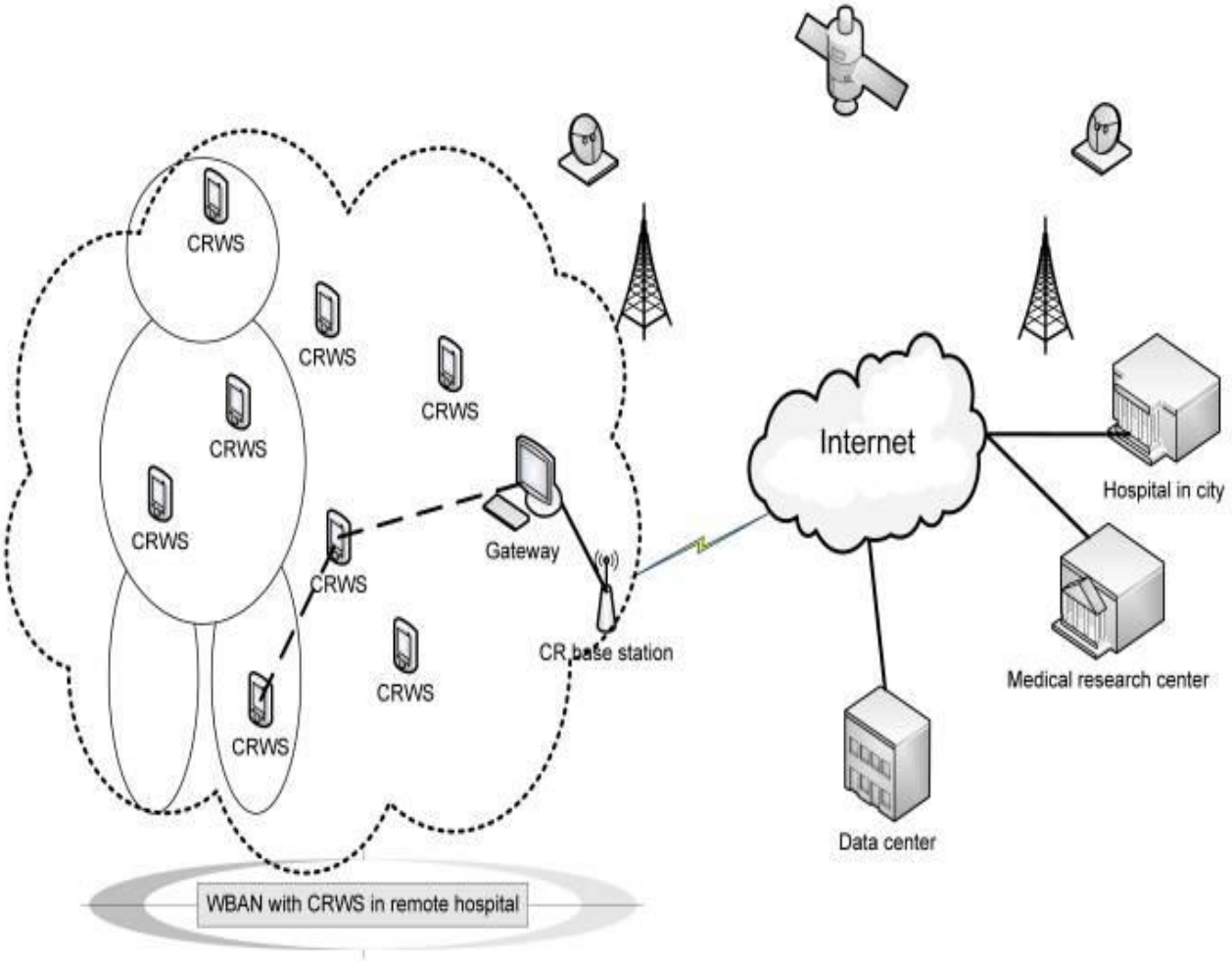


Figure 2.9 : Wireless Body Area Network (WBAN) with CR Wireless Sensor[63].

2.5.5 Transportation and Vehicular Networks

Cognitive radio is one of the most important techniques used in the field of vehicles and transporting applications through monitoring traffic and roads available for transit, for easy tracking of roads by sharing continuous information with drivers to enhance traffic safety and the use of auto cloud computing through the internet. It requires high data security, communications, and query tracking attacks. As shown in the Figure 2.10, it links many vehicles and side and secondary roads that link the different methods of vehicles [64].

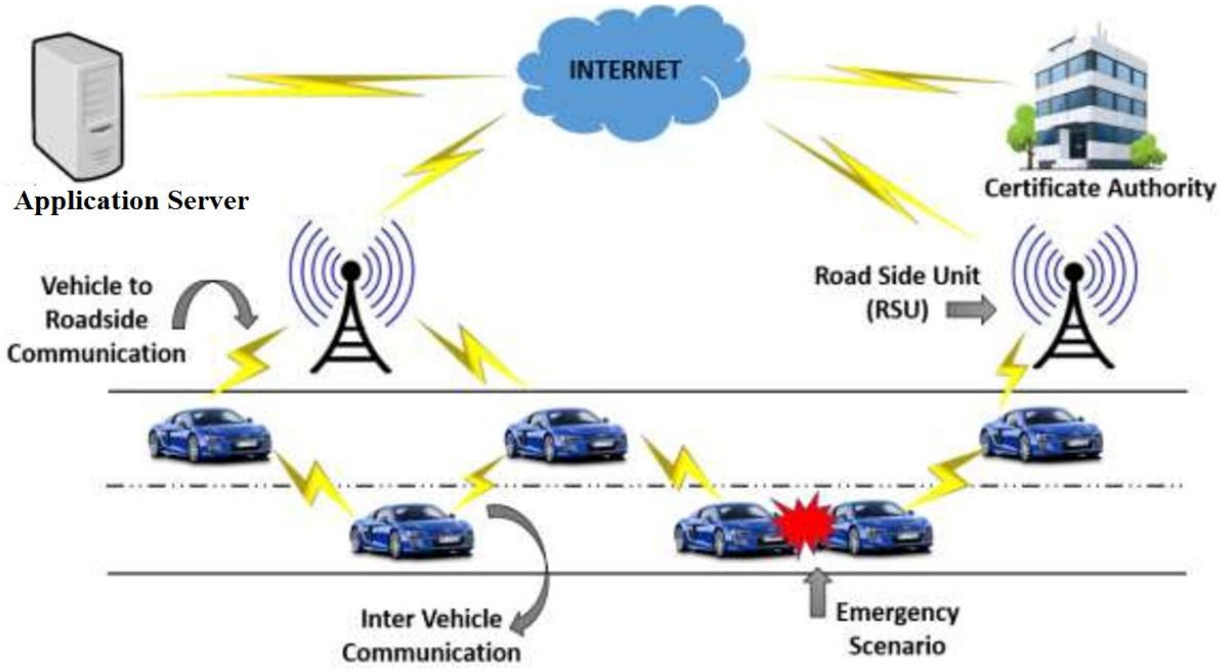


Figure 2.10: Transportation and Vehicular Networks[64].

2.6 Security of Cognitive Radio Networks

As a result of the different fields of the cognitive radio network, which attracted the attention of researchers trends for instance, which addressed issues of routing and spectrum radio sensing and security threats, which require more attention. Of course, security features in the cognitive radio network is similar to security in other types of networks, where security is divided into two parts, the first part is based on preventing attacks from occurring, which is based on cryptographic algorithms, while the second part is based on detecting attacks and identifying harmful behavior and eliminating it after identifying it Thus, it prevents the future attacks happened [65].

The second part is considered more interested by researchers, which is the detection and identification of attacks. Distributed architecture is more challenging to control attacks where the nodes change the position dynamically and more vulnerable to attack than the fixed network. The design of the security system requires the availability of several issues from the attacker's model as it is

taken into consideration to determine the attacker's capabilities and the amount of the impact on the victim [66]. The other issue is the detection methodology, which consists of collecting information from different security sources within the system or outside it, which helps in building the final analysis of the knowledge system to distinguish between normal and abnormal behaviors [67].

2.6.1 Security benefits of Cognitive Radio Networks

The cognitive radio network provided many functions and on various types of applications, especially those that require accuracy in the transmission of information, as well as accuracy at the time to receive information, such as in the case of military applications, and network performance can be improved in the following areas, including security, speed of adaptation, and the use of network resources and son on [68].

Information security is one of the most important factors in the field of networks, especially those that depend on the wireless network. Where security requirements are put in place on the various components of the system at the initial stage, which remains continuous throughout the life of the system, as it reduces the threats caused by accidentally or the threats resulting from human intervention [69]. Due to the importance of the cognitive radio network’s characteristics, for instance, the reconfigurable feature, the network can reconfigure itself according to the requirements determined by the application, and from these requirements is the security of communication by allocating the security level to certain topology resources as this feature reduces delays caused by manual change problems [69].

2.6.2 General Requirements

There are a set of general security requirements that must be taken into consideration when building any security system .Besides, requirements apply to

the main cognitive radio network elements represented by the primary user and the secondary user. The requirements are represented by the following notes [20]:

- The new system must not add new weaknesses
- The system should be able to solve problems (fault-tolerant) and reconfigure itself when problems occur [70].
- The system should be able to detect attacks and indoors vulnerabilities[71].
- The system should be compatible with the requirements of the previous system and at the same time add new detection methods [72].

The cognitive radio network is one of the applications that are based on the wireless open air and therefore it has security problems related to this aspect. In addition to its characteristics such as sensitivity and scarcity of the common channel or the missed location of the primary user, the attacker tries to exploit the weaknesses associated with the layers and protocols within these characteristics. [73]. The security requirements in CR wireless network nodes are authentication , availability, confidentiality, integrity, authorization and non-repudiation [74].

2.6.3 Layered and Cross-Layers attacks Against CRNS

The attacks within the cognitive radio network are represented by the attacks on the five layers of communication as (Physical, Data link, Network, Transport, Application) layers. In addition to the attacks that occur on one of the layers, which may be transferred to other classes, which is represented by cross-layer attacks.

A) Physical Layer attacks

The attacks on this layer are represented by the effect on the physical means that transmit data between the nodes as channel and the attacks carried out on the sensitivity feature depending on the transport medium and the air. CR

differs from the traditional wireless radio network, which based on the Opportunistic Spectrum Access [75].

Many common attacks occur on the first layer of communication within the cognitive radio network, which are represented by the following attacks:

1- **Primary User Emulation (PUE) Attack** : The malicious nodes hide within the network and rely on a specific method to change their behavior to lead to a false sensing operation of the appearance of the primary users[76].

2- **Objective Function Attack (OFA)** : The attacker uses different methods to exploit weaknesses in the techniques of evaluating the parameters on which the network depends on adaptation within the environment, for example, energy, coding rate, bandwidth, and so on, as it leads to a wrong evaluation in calculating the optimal parameters for adaptation, [77], [78].

3- **Jamming Attack** : It is disturbing the communication channels and the desire to stop them by causing denial services and congestion to occupy the communication by processing data other than the basic data that the connection was established for [78].

4- **Eavesdropping Attack** : The attacker listens to the connections between the nodes in the network to obtain information used to build a larger attack[79].

5- **Primary Users' Location Attack** : This type of attack is considered to be the most dangerous attack on the network, as it attacks malicious nodes on devices depending on their location by considering the signal strength to a distance and thus anticipating the site after several operations and then a direct attack on the physical component [80].

6- **Learning Attack (LA)** : The attacker uses the path scattering method for the nodes in the network, as it sends the wrong messages that are transported across the nodes, which leads to the wrong spectral sensing information [81].

B) Data Link Layer attacks

The attacker in this layer tries to exploit the vulnerabilities within the data link layer and within the physical addressing strategies, as shown in the below, the most common attacks are as follows [82]:

1- **Spectrum Sensing Data Falsification (Byzantine attack)** : Attackers of this type attempt to affect decision-making processes after spectrum sensitivity by misleading the use of degraded spectrum holes and reducing the productivity of primary and secondary users in the network [82].

2- **Control Channel Saturation DoS Attack (CCSD)** : This type of attack takes advantage of the network access control and coordination feature, where communication channels allow communication to join in the case of more than one node that wants to connect and be present in the network, and here the malicious nodes try to create fake communication channels to lose control with control channel setting, which leads to reducing the network performance and it leads to congestion with the connection and then stopping it, [83] [84].

3- **Selfish Channel Negotiation (SCN)** : In this type of attack, the malicious nodes refuse to forward the messages coming to them within the guidance to the neighboring nodes to defend the throughput state, which leads to hiding the communication channel [85].

C) Network Layer attacks

The attack on this layer is represented by attacks on defining routing paths for the routing nodes within the network where the malicious nodes create fake paths that help disperse the routing process and reach collision and packet loss [86].

1- **Hello attack** : The attacker uses a high level of power to transmit the routing message to the longest extent on the network, which causes the belief by the receiving node that the signal received is from a neighboring node, which ultimately causes most of the nodes in the network without neighbors for transmission [86].
2- **Sinkhole Attack** : This type of attack aims to assume the best direction contract, especially in the case of multi-hop communication, and therefore the attacker tries to motivate and influence the rest of the contract to choose the optimal path [87].
3- **Sybil Attack** : This type of attack exploits the legitimacy of the contract by reaching the channel, as it uses a large amount of false identities that influence decision-making processes to acquire the degraded spectrum and make the degradation spectrum usable by the imaginary nodes only [88].
4- **Ripple Effect Attack** : The attacker within this type depends on the same strategy to implement before the primary user simulation attack or the Byzantine attack, based on false sensor information where the malicious nodes choose the spectrum ranges for the channel, which may be on the frequency band when converting from hop to hop within the network [89].

D) Transport Layer Attacks

The attacker tries to exploit the vulnerabilities within the connection session, connection utilities, for example direct attack on the communication keys [87].

1- **Key Depletion Attack** : Attacks within this type exploit the many communication establishment processes that within some protocols lead to key duplication, and many protocols that contain this problem have been proven, for instance, the Temporal Key Integrity Protocol (TKIP) and the

Wired Equivalent Privacy (WEP) which implemented in IEEE 802.11. Thus, he takes advantage of this situation until he reaches the key repeat point or the system stopped [87], [77].

2- **Jellyfish Attack** : One of the types of attacks that affect both the third and fourth layers of the routing features and the fourth layer as the establishment of the transport session where it affects the behavior of TCP protocol [60].

3- **Lion Attack** : The implementers of the attacks exploit the transport layer by reducing throughput and exploiting vulnerabilities in a TCP protocol connection [90].

E) Application Layer Attacks

Of course, any attacks that affect the previous layers show their effect on this layer, for instance about these attacks logic errors attack and buffer overflow, while the countermeasure for them as authentication, trusted application and antiviruses [91].

F) Cross-Layer Attack

The distinguishes the cognitive radio network is an application-aware of communication network, where there are various research directions that are based on merging the layers or merging the functions provided by these layers together to reduce unnecessary complexity and reduce implementation time and the requirements of handoff/handover latency of cognitive radio spectrum acquisition [92]. The Figure 2.11, shows the interconnection of Cognitive Radio Sensor Networks (CRSNs) as cross-layer framework based on the main layers as Application layer, transport layer, network layer, data link layer, physical layer and interconnection between them [92].

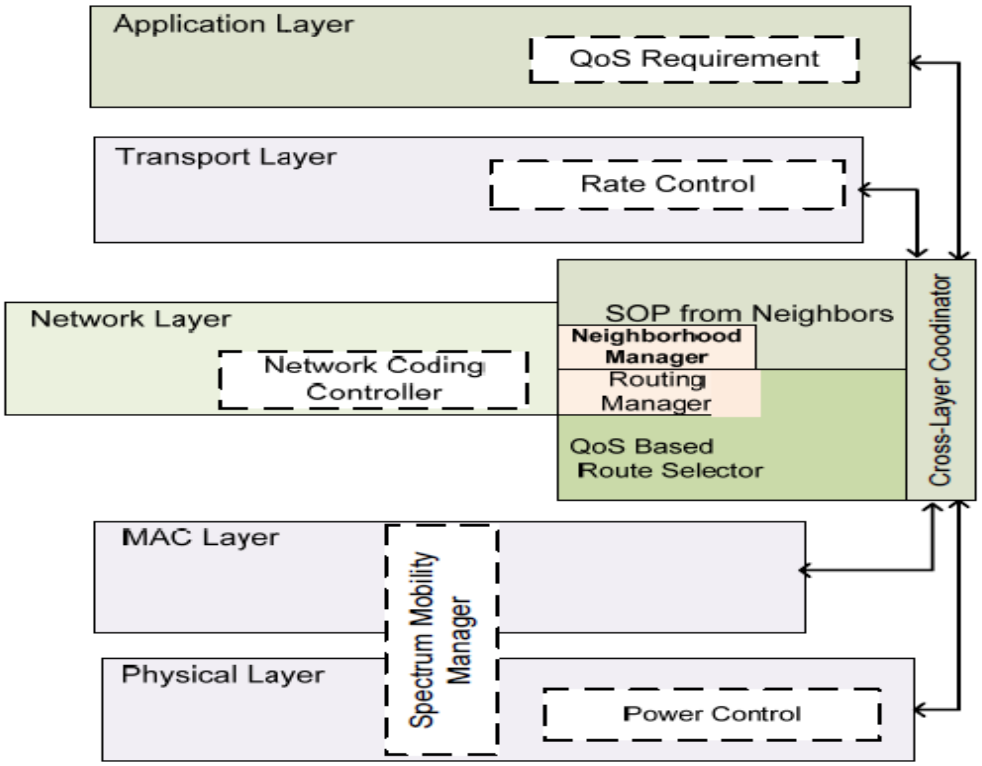


Figure 2.11: Cross-Layer Framework Communications [92].

The Table : 2.1, showed the types of attack on each cognitive radio network layers

Table 2.1: CRNs layer and types of attack on each layer.

CRNs Layer	Types of Attacks
Physical Layer attacks	Primary User Emulation (PUE) - Objective Function Attack (OFA) - Jamming Attack - Eavesdropping Attack - Primary Users' Location Attack - Learning Attack (LA) -
Data Link Layer attacks	Spectrum Sensing Data Falsification -

	(Byzantine attack) Control Channel Saturation DoS Attack (CCSD) - Selfish Channel Negotiation (SCN) -
Network Layer attacks	Hello attack - Sinkhole Attack - Sybil Attack - Ripple Effect Attack -
Transport Layer Attacks	Key Depletion Attack - Jellyfish Attack - Lion Attack -
Application Layer Attacks	Any attacks that affect the previous layers

2.6.4 Security Challenges of Cognitive Radio Networks

There are a collection of challenges facing researchers in the field of developing the cognitive radio network in various directions, including within the five communication layers, including those related to the characteristics of the physical components and most challenges, summarized as follows [93]:

- The consumption of energy.
- Computation power of the hybrid system.
- Spectrum sensing reliability, analyzing, mobility, and sharing.
- The security of CR communications schemes.
- The radio resource allocation management [93], [94], [95] .

2.6.5 Still Open Problems

There are a group of issues that have been mentioned in various academic researches and have been classified as problems that are still pending or considered open issues for development and modification. Among these issues that we have summarized are as follows [96]:

- Disclosure of the malicious nodes activity [96].
- Improvement security and privacy Frameworks [97].
- CR spectrum sharing-allocation of the Internet of Things(IoT) applications [98].
- QoS within the transmission requirements of the CR-MAC layer [99].
- Energy-efficient of mobility spectrum sensing [99].
- Malicious Users identification of Cognitive IoT Networks based Genetic Algorithm [100].

2.7 The used secure Cognitive Radio Network System components

The proposed system based on the three simulation parameters where, Throughput is described as the ratio of the number of packets received to the total number of packets sent, and the equation used as [23] :

$$Throughput = \frac{\text{Number of Recieved Packets}}{\text{Total Number of Sent Packets}} \qquad [23]$$

Data Drop Rate is represented as the ratio of the difference between the total number of packets sent and the total number of packets received to the total number of packets sent, and the equation used as :

$$Data\ Drop\ Rate = \frac{\text{Total no.of Sent Packets} - \text{Total no.of Recieved Packets}}{\text{Total Number of Sent Packets}} \quad [23]$$

Detection Tim is determined as the difference between the time of the detected channel and the time the sensing of the channel started which are defined as the finishing time and the starting time respectively. Through, the time used to hop from one channel to another about 400ms, which is described as the Dwell time of frequency hoppy.

Once the dwell time has terminated, the system operation hops to another channel within the proposed available channels of the used ideal channels pool.

$$Detection\ Time = Finishing\ Time - Starting\ Time \quad [23]$$

While the delay time is the time used to transmit packet from the sender to the receiver and it explained the delay time simulation parameter for entire packets. It computed based on the following equation :

$$d_{trans} = L/R \quad [121]$$

Where the d represents as the delay time in seconds and the L, as the packet length in bits and the R as the rate of transmitted data in bits per time unit.

2.7.1 Frequency hopping spread spectrum (FHSS) used in Cognitive Radio Network

The used algorithm based on Frequency hopping spread spectrum (FHSS) to enhance cognitive radio parameters within the simulation parameter. FHSS is the repeated switching of frequencies during radio transmission to reduce

interference and avoid interception. It is useful to counter eavesdropping, or to obstruct jamming of telecommunications, and it can minimize the effects of unintentional interference [101]. The FHSS algorithm makes the transmitter hopping between available narrowband frequencies within a specified broad channel in a pseudo-random sequence known to both sender and receiver. A short burst of data is transmitted on the current narrowband channel, then transmitter and receiver tune to the next frequency in the sequence for the next burst of data.

Because no channel is used for long, and the odds of any other transmitter being on the same channel at the same time are low, FHSS is often used as a method to allow multiple transmitter and receiver pairs to operate in the same space on the same broad channel at the same time. The used method for frequency hopping technique estimates as (2.22 GH, 2.24 GH, 2.26 GH , 2.28 GH , 2.30 GH , 2.32GH , 2.34 GH , 2.36 GH , 2.38 GH , 2.40 GH , 2.42 GH , 2.44 GH , 2.46 GH , 2.48 GH , 2.50 GH , 2.52 GH , 2.54 GH , 2.56 GH, 2.58 GH, 2.60 GH) frequency bands, through these twenty bands, applied as twenty channels. So, it is clear the function of the first layer (Physical Layer) through send and receive signals from CR-node to another node and create the information that will be passed to the second layer by proposed interfaces called (upper, lower) interfaces known as Control and Data exchanges interfaces. The proposed algorithm of spread spectrum technique (FHSS) has a range of frequencies as twenty frequencies bands described as the (idle channel) for transmission suggested by the Spectrum Sensor module of the used system within OMNET++. If misconduct or collision (interference) occurs on a given channel frequency after arrived at specific threshold value, which it determines as interference, it will hop to another frequency band selected from the frequency pool(twenty channels) based on algorithm parameters for the proposed channel and data channel. So this feature makes the proposed work more reliable and secure against security issues (interference) and more effectual for the used system parameters(throughput, data

drop, detection time). The Figure 2.12, illustrated the block diagram for the proposed (FHSS) spread spectrum technique to access the twenty idle channels.

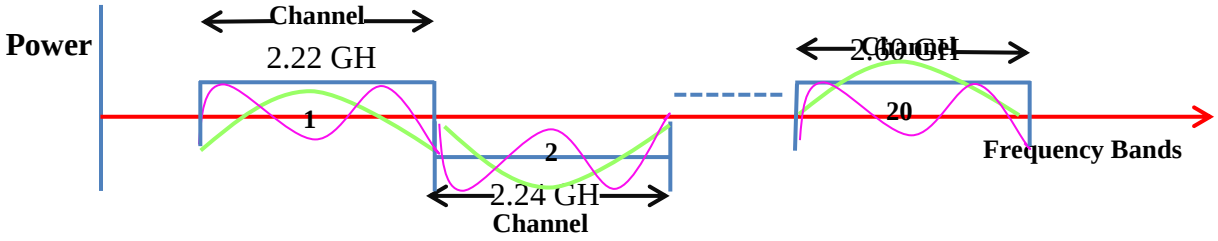


Figure 2.12: The FHSS switching among Proposed Channel.

The Figure 2.13, shows how the channel is exploited in an opportunistic manner by main cognitive radio network elements Primary users and Secondary users and how they can access for each frequency band channel from cognitive users without harmful licensed user when acknowledge channel is busy and should not use by cognitive users. Which mean the ideal transmission state of cognitive radio users be carefully not access to collision state. Busy and Idle states describe the presence and absence intervals of primary user sequentially. The secondary user can obtain the radio spectrum of the idle state of primary user because busy state represent working interval or presence PU.

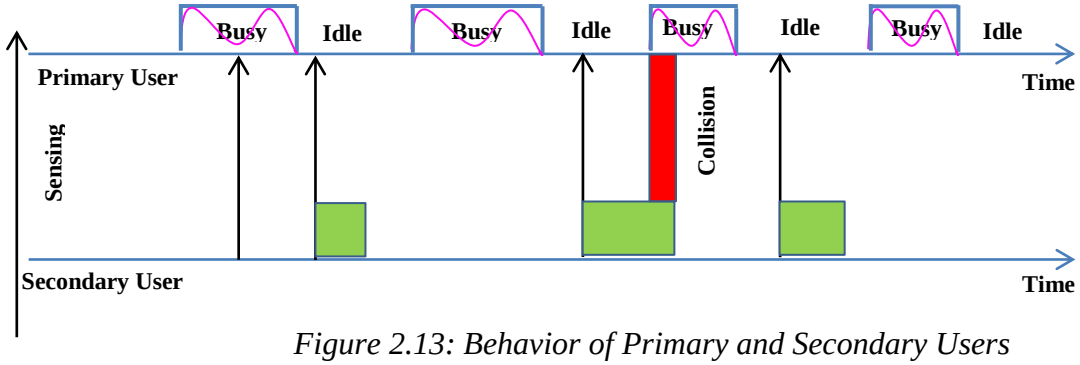


Figure 2.13: Behavior of Primary and Secondary Users

2.7.2 The used Encryption Method (RSA)

The Rivest-Shamir-Adleman (RSA) algorithm is one of the common secure public-key encryption. It is considered one of the important algorithms in maintaining the security of the cognitive radio network, as well as dealing with

many security problems and attacks by ensuring the integrity of data transmission and authorization features in the network [102].

Using an encryption key (e,n), the algorithm is as follows:

- The message is represented as an integer between 0 and (n-1).
- The message Encrypted by power module N to get cipher-text message C.
- To decrypt cipher with power d module n.
- The encryption key (e,N) is produced public. The decryption key (d,N) is maintained privately by the user.
- The encryption process with Public Key.
- The decryption process with Private Key / secret key.

The sender encrypts the data by applying a public key of the receiver and employs an encryption algorithm that is also determined by the receiver and the receiver sends only the encryption algorithm and public key.

In the public key, data does not decrypt so the public key used for encrypting process, While the private key used for decryption process that only the receiver has. So no one can hack the transmitting data [103]. The procedure for producing public and private key in RSA explained as follows:

1- Choose two prime numbers as p and q.
2- A modulus (N) is measured by multiplying (p) and (q) as (N=p*q). which is handled by both the public and private keys and produces the connection between them. Its length, usually represented in bits, is named the key length.
3- The public key of RSA (N, e) where e public key index.

The process of Encryption rounds explained as following [104]:

- Capturing the recipient public key (N, e).
- Describing the plaintext message as a positive integer M, 1 < M < N

Computing the cipher-text C(cipher) = M(plain-text) e mod N as :

$$(C = M^e \ mod \ \text{N})$$

- Transfers the cipher-text C to the receiver.

While, The Decryption process specified as following:

- Using the private key (N, d) to compute M(plain-text)= C(cipher) d(private exponent) mod N as :

$$\text{M} = C^d \ mod \ \text{N}$$

- Obtaining the plaintext of the message representative M [104], [105].

The used system based on the RSA to encrypt and decrypt data as explained in Figure 2.14.

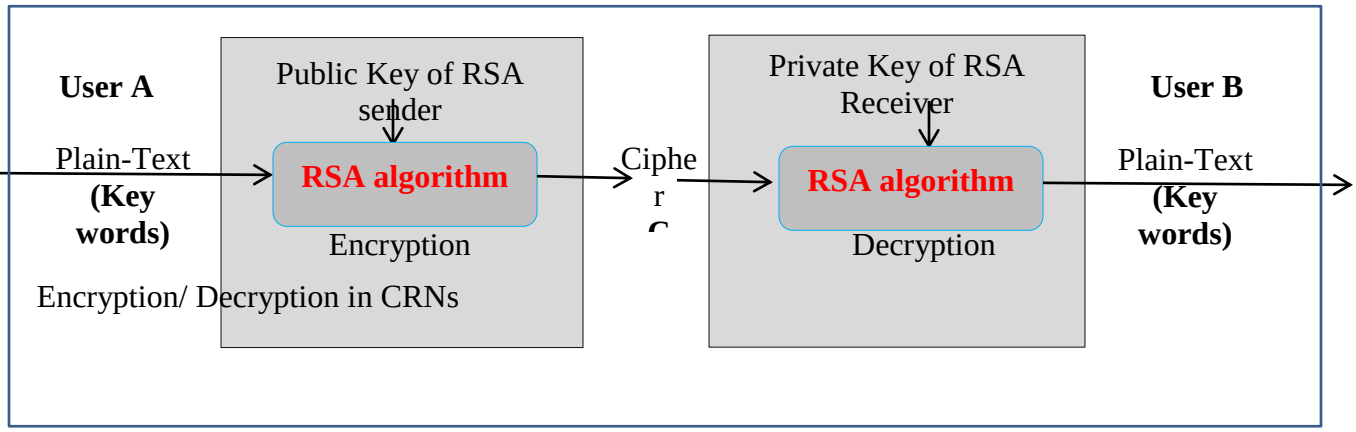


Figure 2.14: RSA Block Diagram for The proposed System.

For example about the encryption process of RSA using the public key that has been established previously e = 7 based on the formula [105]:

$$C = M^e \ mod \ \text{N}$$

For example, we will take " ICENIS" as the numbers with (736769787383) as the Plain text so the explanation steps as follow:

1- Determining the two prime numbers, with the names

p and q. Suppose the value of p = 51 and q = 5.

2- Calculating the modulus value (n):

n = p * q

n = 51 x 5 so n = 255

3- So, From the previously described steps, the values n, e, and d have been obtained so that the key pair has been formed.

- Public key pair (n, e) = (255, 7)
- The secret key pair (n, d) = (255, 343)

4- RSA encryption process with :

I : it means I have a value of 73 within the value of the ASCII table

C : it means I have a value of 67 within the value of the ASCII table

E : it means I have a value of 69 within the value of the ASCII table

N : it means I have a value of 78 within the value of the ASC II table

I : it means I have a value of 73 within the value of the ASCII table

S : it means I have a value of 83 within the value of the ASCII table

The encryption process by using the public key from RSA, which has been formed before that as a value of "7 pieces" , using the formula : $C = M^e \ mod$ N. [105]

73^7 mod 255 = 112 , which it equal to the ASCII table value as p

67^7 mod 255 = 118 which it equal to the ASCII table value as v

69^7 mod 255 = 69 which it equal to the ASCII table value as E

78^7mod 255 = 192 which it equal to the ASCII table value as ʟ

73^7 mod 255 = 112 which it equal to the ASCII table value as p

83^7 mod 255 = 212 which it equal to the ASCII table value as ⊾

5- While the Decryption process of RSA based on the private Key is d=343 and the result values as follows:

$$M = C^d \ mod \ N$$

$112^{343} \ mod \ 255$ = 73 on the ASCII table I

$118^{343} \ mod \ 255$ = 67 on the ASC II table C

$69^{343} \ mod \ 255$ = 69 on the ASC II table E

$192^{343} \ mod \ 255$ = 78 on the ASCII table N

$112^{343} \ mod \ 255$ = 112 on the ASC II table I

$212^{343} \ mod \ 255$ = 83 on the ASC II table S . [105]

2.8 Simulation tools used to enhance security of Cognitive Radio Network

In addition to the real implementations of the cognitive radio network, there are many simulations, programming languages, and frameworks that allow the possibility of applying this network and various research directions, especially in the field of security of cognitive radio networks as in the simulations tools mentioned in the below:

MATLAB: It is the most accessible and most productive software to simulate a different type of network security architecture for example, in [93] the author suggested game-theoretic strategy within mobile ad-hoc networks to evaluate the security performance goal and power consumption. While in [106] it implemented the Markov chain theory to analyze the performance of CRNs as anti-jamming model.

NS-2 : It is considered one of the most important simulation tools that are used in the field of networks in general and cognitive radio networks in special, where it is applied in the field of security to simulate the risks and malicious nodes and others.[93], for example, it is used trust structure to identify Malicious Nodes in

CRNs through guaranteed a trusted way for data delivery based on the Tidal Trust Algorithm (TTA) [107].

NS-3 : It is one of the developed open-source versions of the NS2 simulator. It contains numerical simulation frameworks appropriate for different types of networks and their applications as it is widely used in the cognitive radio network field to detect the primary user and sensitivity to the radio spectrum as well as security areas [108]. It used within [109] for heterogeneous cognitive network within mobile Cognitive Radio Networks, and in[110], it used for spectrum sensing techniques for handoff/hand over and PUs detections within smart environments.

OMNeT++ : It is considered one of the open-source simulators, which is characterized by the ease of installation and learning, as it is one of the simulations that it has many used the field of information technology as one of the most important academic tools because of its easy-to-use GUI interfaces and application as well by adding extension tools attached to the implementation of the cognitive radio network such as Castalia and Simulink [111], it used in [112] for authentication mechanisms and digital signature design employed a specific CRNs hash function, to identify security requirements such as data authentication, integrity, and non-repudiation of the primary and secondary users in CRNs.

OPNET : It provides many benefits to the cognitive radio network, as it depends on an easy-to-use graphical user interface and depends on it to implement, develop and modify various algorithms in the field of networks, including allowing data filtering and infiltration detection from penetration and detecting network weaknesses[113]. While, Real-time Spectrum management strategies for CR with MAC within the implementation of industrial WSNs implemented with OPNET simulation tool [114].

Qualnet : It is used to develop and manage different network communication systems, for instance, it used to simulate the security threats and privacy protocols for specific Cognitive Wireless Sensor Networks(CWSN) to evaluate the effectiveness of jamming attacks and the impact of jamming within control protocols (UDP, TCP) [115].

In [116] used Qualnet for the spectrum selection analysis approach within a cognitive radio network to apply control of the channel within Dynamic Spectrum Access (DSA).

Monte Carlo : It is considered one of the simulations used to study the effect of security risks in the field of communications and information networks and cognitive radio networks so it used to simulate the cooperative spectrum Sensing [117]. Also, it implements the concepts of optimized sensing to enhances the signal to noise ratio (SNR) within the detection probability performance[118].

While in [119] it used to verify the availability of the suggested algorithm with various possibilities of security threats from malicious users within cognitive radio networks of spectrum Sensing within a centralized System.

COOJA : It is a one of the open source simulator which is based on java/c core implementation, It based on the sensor module, so it is used to apply some of the attacks that affect wireless sensor networks, such as a Sybil attack and cognitive radio networks [120].

Besides, there are many simulation tools used to simulate different approaches within cognitive radio networks, for example, J-Sim, NetSIm and so on. There are different simulation tools because it has many research directions on various parts of the network and even at the level of application of the network, for example, there are research directions regarding the first layers (Physical layer, data link layer) of communication and others regarding the routing features as the

network layer, etc. Also, the diversity of the cognitive network applications made this diversity in the application tools of CRNs simulators and programming languages. Table 2.2, shows general simulation tools and the core programming language used that can apply to achieve cognitive radio networks.

Table 2.2: Cognitive Radio Network Simulation tools and Official Websites.

Simulation-Tool	**Official-Website**	**Core programming language**
MATLAB	https://www.mathworks.com/	C, C++, C#, Java, Fortran and Python
NS_2	https://www.isi.edu/nsnam/ns/	OTcl, C++
NS_3	https://www.nsnam.org/	Python, C++
OMNeT++	https://omnetpp.org/	C++, Java, C#, NED
OPNET	www.opnet.com	C, C++
Qualnet	http://www.qualnet.ca/	Parsec, C++
MONTE CARLO	http://www.goldsim.com/Home/	JavaMonte
COOJA	http://www.contiki-os.org/	Java/C
J-Sim	https://www.physiome.org/jsim/	Java
NetSIm	https://www.tetcos.com/	Java/C

CHAPTER THREE

A developed Cryptosystem for Cognitive Radio Networks

3.1 Introduction

Cognitive radio (CR) is a spectrum dynamic manner technology which considered a modern method for enhancing the spectrum utilization within the wireless environment. It's produced based on the concept of a software-defined radio as well as, represented as a smart wireless communication method that is aware of the surrounding environment. The cognitive radio uses the methodology of understanding and learns/discovering from the environment to particular parameters, furthermore, it changes in the input parameters stimuli that are affected by the decision-making process for selecting the best idle available channel. CR implements in various types of applications, for instance, CR-Leased Networks, CR-Emergency Network, Intelligent Roadside, Safety, Vehicles Network, Cellular Networks, Multimedia application, and the most important application is the military application where cognitive radio play as an excellent service within this application [122]. This study is developing a Cryptosystem to enhance the security of CRNs by implementing:

- Public-key cryptosystem of Rivest, Shamir, and Adelman (RSA) type.
- Using spread-spectrum techniques such as a Frequency hopping spread spectrum (FHSS).

Enhancing Cognitive Radio (CR) with the main simulation parameters used such as the (Throughput, Data Drop Rate, and Detection Time). All the simulations implement in OMNET++ simulation tool and visual C# language.

We choose OMNET ++ because of it's easy to use with (Tkenv) Graphical User Interface (GUI) for the windows operating system. This GUI provides different features of tracing, debugging and execution:

1- It's recommended in the main development simulation stage since it allows to get a detailed picture of the simulation state at any point of execution timeline.
2- It is a modular with different (Frameworks, Libraries, Models, etc.) which save time and effort for researchers to carry out research simulations like the real environments.
3- Following what happens inside the network.
4- The flexibility of learning where it depends on C ++ programming language.
5- OMNET++ graphical user interface based on NED topology description language which its trace what happens inside the network .
6- The lack of requirements for the installation state in Windows operating system. According to the general network architecture of Cognitive Radio Network, all the communication takes place on the primary-secondary user model where primary users act as a base station and secondary users as military application units.

Many processes are done to build and execute C++ code within Omnet++ simulator, where it based on different simulation parameters that come from a different files header and source and initial files and supporting file for core messages and network description files.

The Figure 3.1, shows Omnet++ building and running programming steps, the main classes and objects as the MSG Files(Messages Files), OPP_msgc (message compiler), _m.cc (message source files), NED File (Network Description File), Omnetpp.ini (Initial file for OMNET++) .

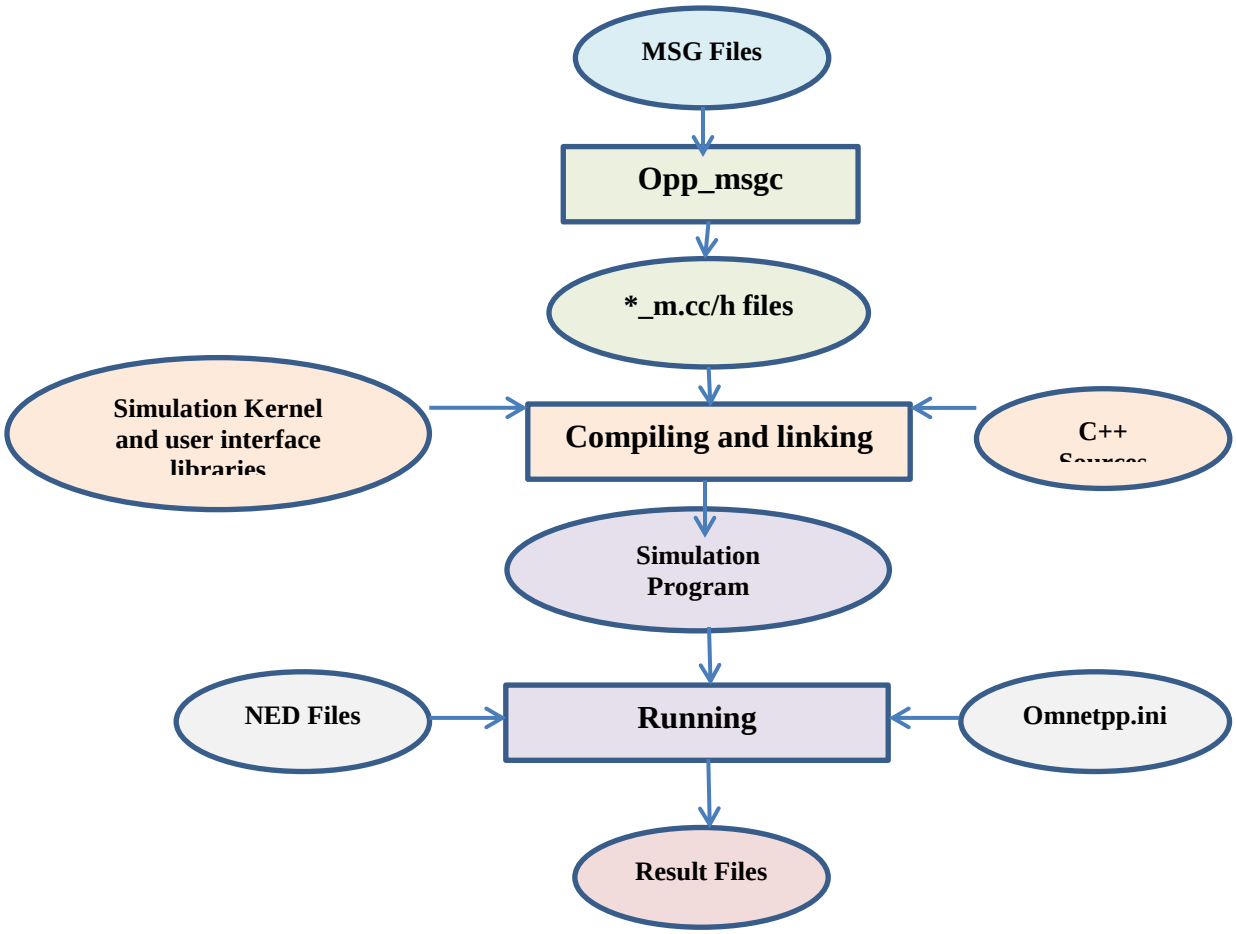


Figure 3.1: Omnet++ Process and Running Code Steps

3.2 Cognitive Radio Network Architecture

The architecture of the Cognitive Radio Network is similar to most types of wireless networks architecture based on the five popular communication layers for sending and receiving data as well as various data types like text, sound, and video since the proposed systems based on (**Text**) data type .

The practical side of each of these modules as C++ core for OMNET++ simulation code will be representing for each system module. The used system description in each layers (Application Layer,Transport Layer, Network Layer, Data Link Layer, Physical Layer) as following [123]:

3.2.1 Application layer

It does not send real data. Instead, it used only a request signals through the layers lower to the MAC layer. The MAC Layer creates a random amount of data packets (specified in **.ini file)**: its allow giving values of parameters during initial time which are effect later on overall simulation execution ,on the other hand, experimenting with the model by running it several times with different parameters.

It is important to clarify the parameters that are expected to change (or make sense to be changed) during experimentation should be put into ini files.) and attempts to send it to a destination. As well as, it creates a random amounts of transmission data depending on the settings in the configuration file. Furthermore, , it collects the successful and failure communication statistics based on the signaling feature. The Figure 3.2, shows the main steps of the used application layer. The used application layer based on the two stages or phases showed as the initial stage responsible about initializing or definition simulation parameters values which they passed from lower layers and the handler stage responsible about data signaling process and how to deal with them.

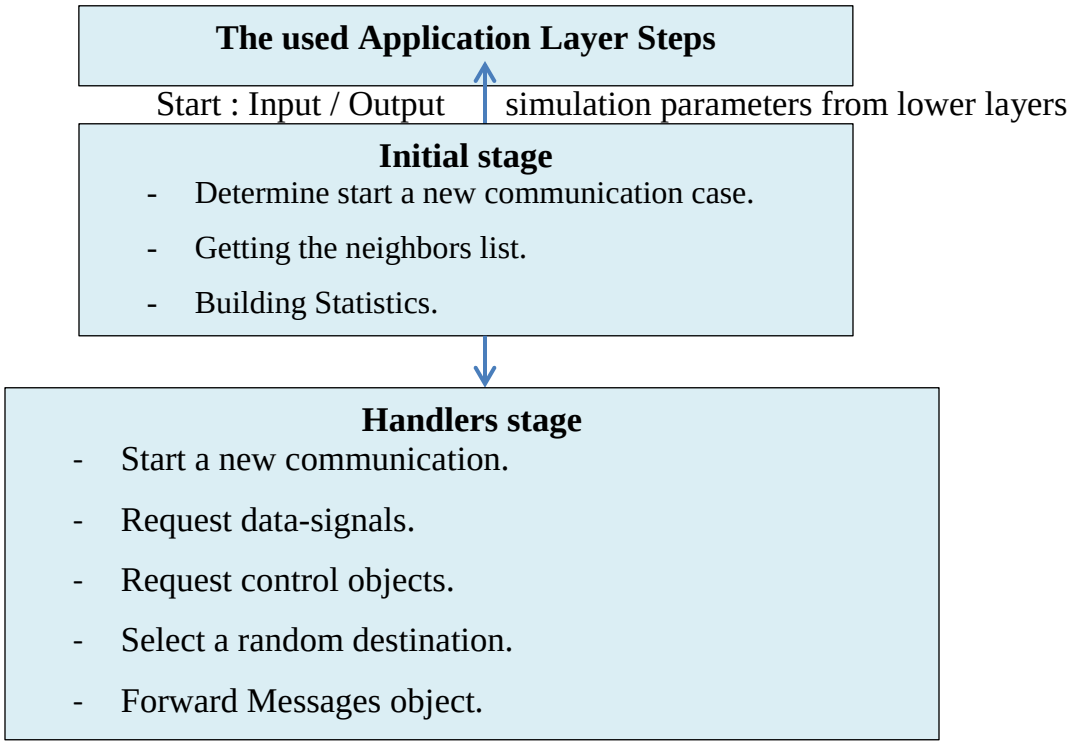


Figure 3.2: The proposed Application Layer.

3.2.2 Transport layer

The implementation of transport Layer as a "pipes" for information represented by Data_messages and control_messages. It is responsible for establishing session for host to host transmission.

3.2.3 Network layer

The main job of this layer is routing like other traditional network layers so it controls on data coming from upper and lower layer through interfaces to determine destination of packets. So, it selects a random destination node among its one-hop peer nodes in the network. The addresses (source address(own address) and destination (neighbors)) of the one-hop neighbors need to be provided in the topology (.NED) is a file of the network under (address, neighbors) parameters. The folder CrNetworks contains root network description file(.NED). Which is responsible executing project and collect all classes and methods from other directory as supporting packages we invoke them through namespaces section. In addition, general parameters like sub-modules (address, neighbors, etc.) and full-duplex connections among nodes. Overall steps are represented by the Figure 3.3, as procedures of behavior of the used network layer.

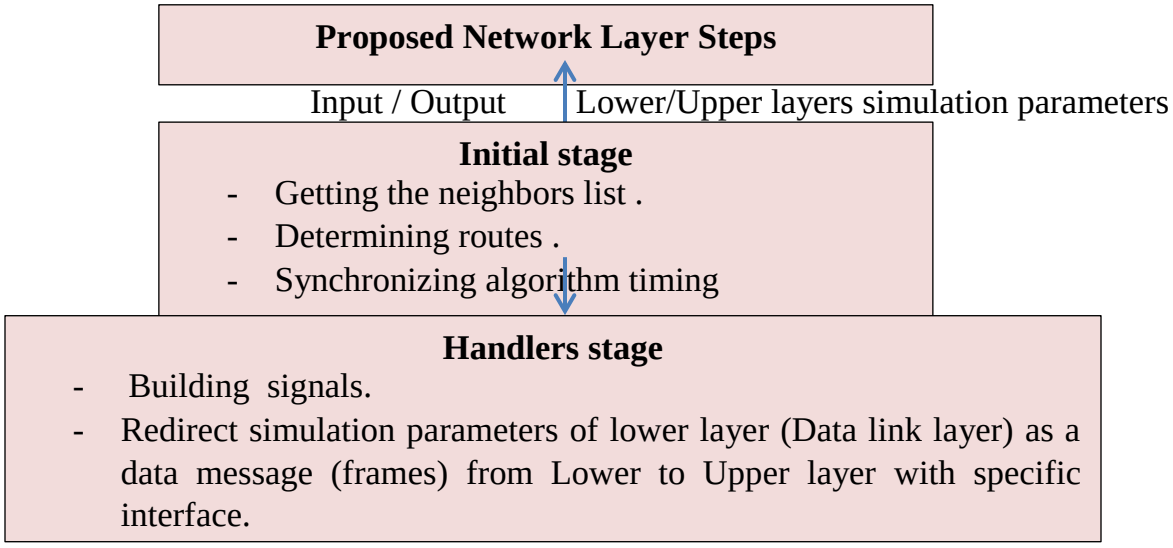


Figure 3.3: The used Network Layer Algorithm.

3.2.4 Cognitive-Radio-MAC-Layer

Medium access control is responsible to accomplish tasks related to the smart behavior for selecting the spectrum bands and encapsulation frames for security purpose as well as the mobility feature.In addition, provide additional specific feature not found in traditional wireless networks.

Through, dynamic channel accessibility, and channel handoff /handover mechanisms with a spectrum sensing provided information about the events of available channels, through selecting the best channel for communication according to a set of parameters that decide efficiency CR-MAC protocol. In addition, the proposed system implemented CSMA (RTS, CTS) based MAC protocol with channel dynamically access.

This configurable protocol has many parameters can change through the configuration file.It deals with simulation parameters of data type incoming from physical layer and pass to network layer.

It deals with simulation parameters of data type incoming from physical layer and pass to network layer with specific function of the used system known as [send()] method which is called message based on the different procedures.

The initial state of the data link layer algorithm it describes starting point to get parameters values, while processing state or algorithm body is based on the handler function as the main function of data link layer to building simulation objects and passing frames or data signals to build the results within MAC layer

The Figure 3.4, shows the main steps of using MAC layer with the different setting for incoming/outgoing objects between lower/upper layers. The proposed setting starts with the incoming signaling from physical layer and then deals with the building data link layer frames encapsulation configuration and then pass the data signals to the upper layers.

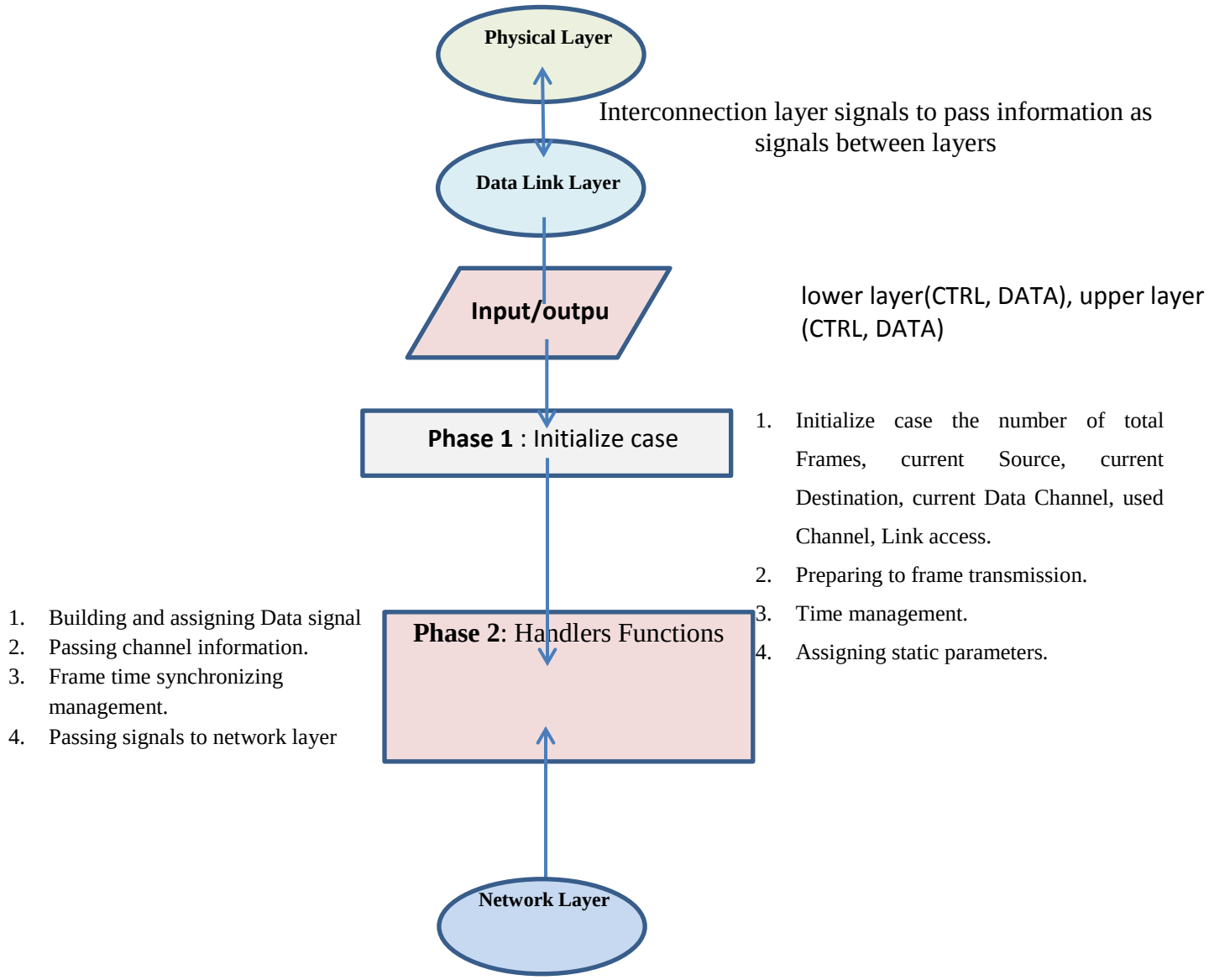


Figure 3.4: The flowchart of the used MAC-layer algorithm.

3.2.5 Physical layer

The main job of this layer is concerned with the physical component features and channel proprieties. It receives messages from all connections/channels through any physical layer parameters need to be appended to the outgoing messages. This feature provides dynamically alteration for implementaion parameters without required to change the transmission to a new

NIC module. Another important feature added to this layer from the proposed system using adapting method based on spread spectrum technique Frequency Hopping Spread Spectrum(FHSS) as (twenty frequency bands) to eliminate interference and jamming attack with dynamicaly change current data channel after sensing another idlle channel (proposed channel) with another channel band.

So, within the used approach of cognitive radio network can calculate the data signals (Frames) that arrived without error to the receiver on each reception node, and evaluating the quality of the proposed system by using message statistic test which determines how many messages scheduled through overall simulation time for all cognitive radio network nodes. Besides, we can determine the number of channels available for users and idle one suggested from the adapting method of FHSS. We illustrated physical layer algorithm steps within the cognitive radio network in the Figure 3.5.

Proposed Physical Layer Algorithm
Input/output : Address, Control Upper, Data Upper, Sensing Spectrum Interface -(Upper Layer Parameters)
Phase 1 : Initializing transmission parameters - Building simulation interfaces to connect network elements. - Assigning physical address for node identification.
Phase 2 : **start handleMessage function** **Case 1**: if Control message (RTS/CTS) from Data link layer msg->arrivedOn("ctrlUpper$i") *\ arrivedOn : Boolean method return true if match value for any vector gate. **Case 2**: if Data message from Data link layer - Sending it to destination node through data rate spectrum module as: - msg->arrivedOn("dataUpper$i") - dataMsg *recMsg = check_and_cast<dataMsg *>(msg) - broadcast(recMsg); *\ A check_and_cast<> that accepts pointers other than cObject. **Case 3**: Sensing information arrived through Spectrum sensing interface message deliver

to data rate Spectrum module with :
- msg->arrivedOn("ssInterface$i)

Then (received Message, "dataUpper$o");
Else if Control Message and determine that with Control class then send it for sensing process :
send(copy, "ssInterface$o");

Phase 3 : **broadcast**

-Send data messages arrived for all interfaces (ports) with output array as:

Loop : for (int x=0; x<gateSize("radio"); x++)
{ Data Message *copy = (data Message *) message->dup();
send(copy, "radio$o", x); **}**

*\ gateSize: Returns the size of the gate vector with a specific name among brackets. (1) for non-vector gates, (0) for doesn't exist gate or the vector has size 0. gate names also accepted with "$i" or "$o" suffix.

End Algorithm

Figure 3.5: The proposed physical layer Algorithm.

While the used FHSS library in C++ within OMNET++ contains on the main objects will be described as follow:

INET library : It is a Framework installed and uploaded as an open-source OMNET++ scheme for different wired, wireless, and mobile networks it contains on different features for OSI-layers, communication protocol implementation, routing protocols features and it supports various networking topics.

FHSS- Gaussian Frequency-Shift Keying (GFSK) library: it describes the used GFSK modulation architecture based on the C++ library for OMNET++ and we use it as a standard library for this modulation/demodulation purposes without changing on the setting of this tool for bandwidth, frequency deviation, and modulation index setting.

FHSS preamble modes : it contains synchronous features for the selection control antenna setting. It applied as a frequency library, in addition to preamble data as a start frame delimiter to define the start point of the frame.

FHSS Header modes : It contains signal header modes as the rate, length, parity- reserved and tail fields which specified as the common fields implemented with C++ code behind. *FHSS Data modes with 4GFSK modulation*: It contains the common 4GFSK modulation and demodulation features for bit generator, Gaussian filter and another setting as an open-source library used within OMNET++ namespace library [124]. The proposed system simulated in the (Physical layer) and (Data Link layer). There are another modules as supporting schemes for the proposed work through interconnection and signaling exchanges among layers

3.2.6 The supporting Battery Module

The purpose of this modules is to provide power awareness. It receives a direct signals from CR architecture and then reduce the abstract battery level for power control based on interconnection signal. The Battery Power unit effected with the system processes as cmputation power processes within Radio frequency units, Processor, Memory and sensing Units. Feature (power awareness) exploits to avoid misbehavior caused de-synchronization among nodes and affected on spectrum sharing which lead to prevention Selfish attack [125].

3.2.7 The supporting Statictics Module

This module used to collect and extract statistical results related to various variables within layers of cognitive radio nodes architecture. Its objects (cStatictic subclasses such as cStdDev) generate several lines: mean, standard deviation, and so on, by using the vector, scalar and histogram statistics to explain the results.As well as simulation results have affected based on these modules and

each algorithm implemented to simulate real work for each concern and give the same behavior for the actual module. Noteworthy, Mobility isn't simulated in the proposed system in contrast it is based on fixed topology. Each of these modules in the fixed topology will be illustrated in the Figure 3.6, and their interconnection among layers as control link and data link to provide reasonable results based on statics module and simulation parameters [126].

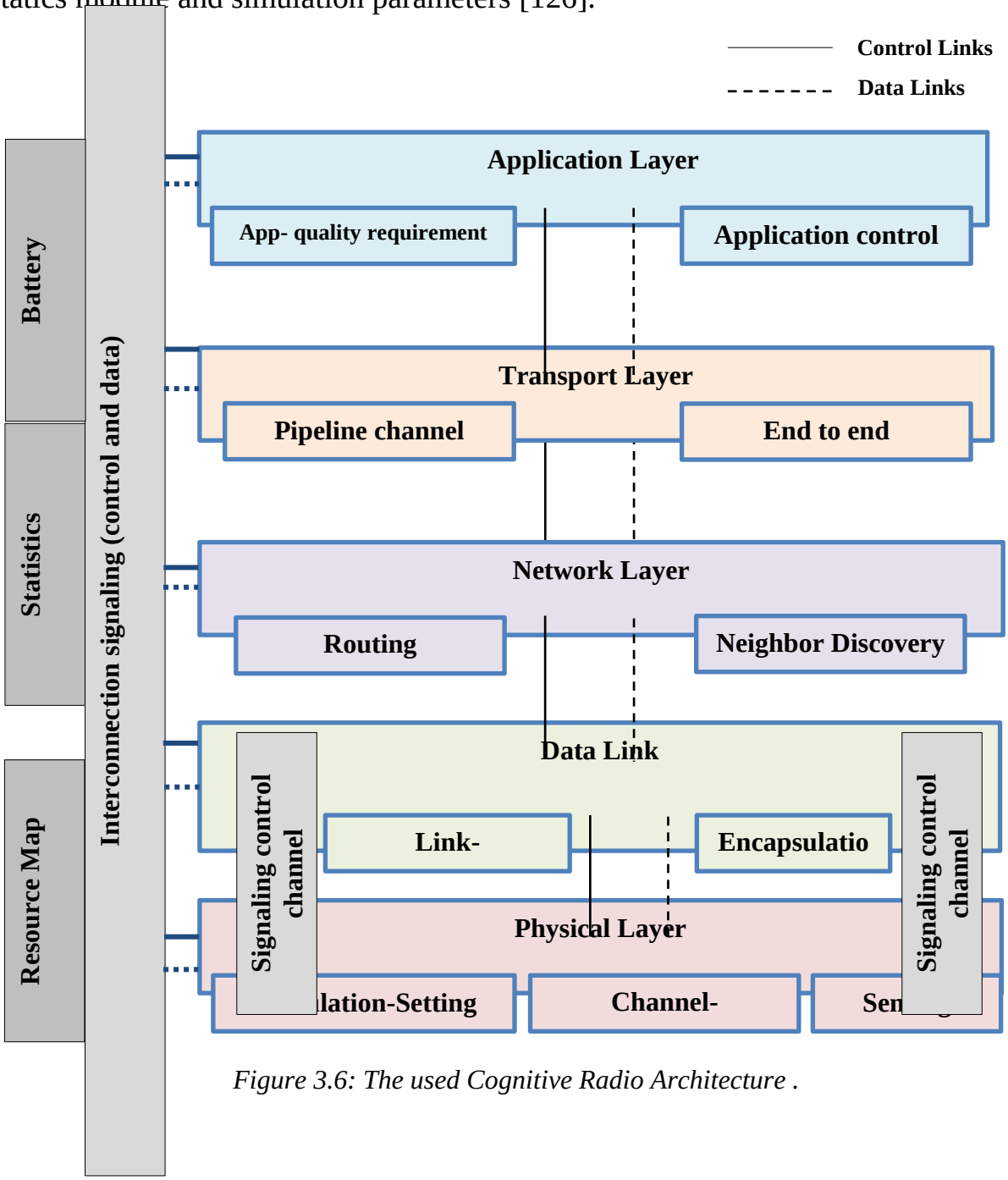


Figure 3.6: The used Cognitive Radio Architecture .

3.3 Interconnection Links used in Cognitive Radio Network layers

The practical side of each of these modules as C++ code will be explore using our parameters assumed during work for each section.

The proposed system based on C++ because it is the core of building libraries and OMNET ++ based on it. The main benefits of interconnection link functions is shown in the Figure 3.7.

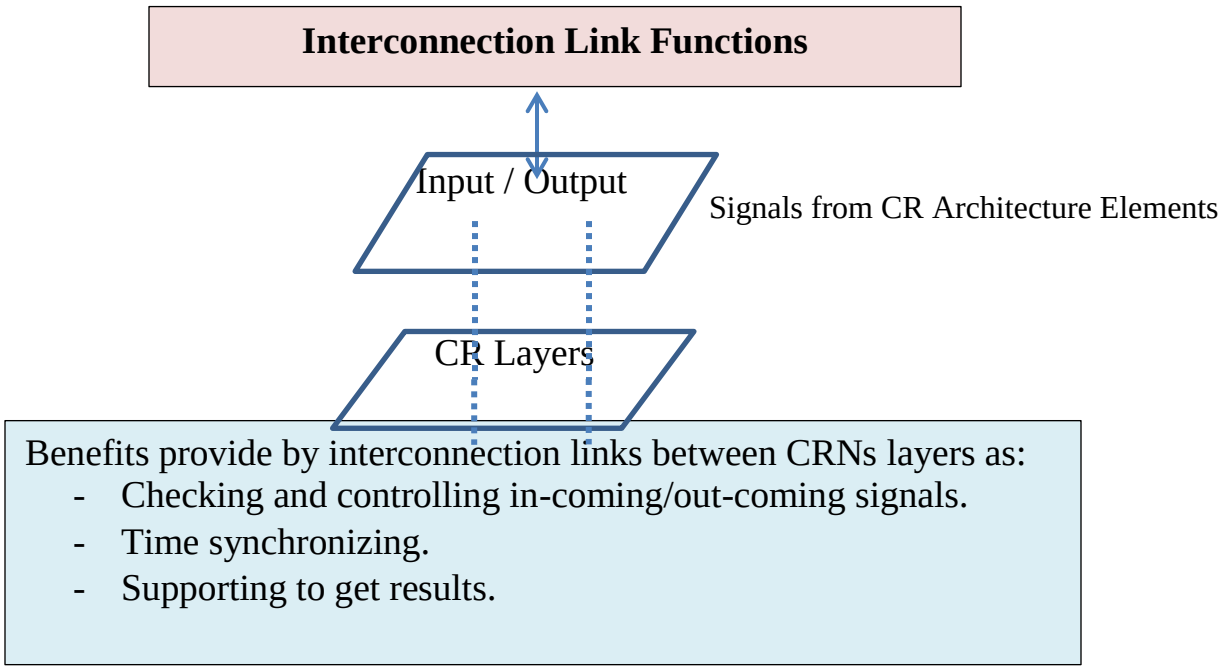
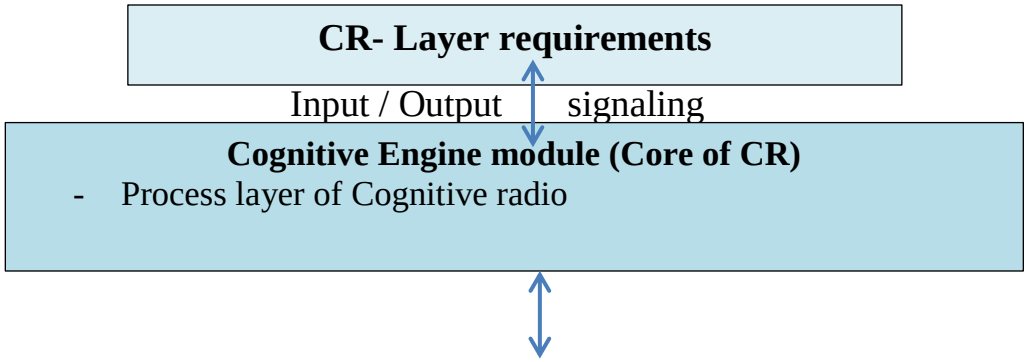


Figure 3.7 : The Interconnection Link Functions

Cognitive Engine & Resource Map Modules: This module contains source and header files responsible for interconnection layers and supporting signaling and communication module through core and CrNodes [126]. These modules used for knowledge aggregation and decisions produced from signaling and communication(interconnection among layers)that's later employ to build statistic results, as they showed in Figure 3.8 .



Software adaptable layer controls

- Acting for learning engine
- Observing knowledge base

Figure 3.8: The proposed Core Cognitive Engine Module.

CrNodes Module : It contains the layer structure and their interconnections like signaling and communication links, statistic and cognitive engine. Moreover the initial default parameters and their data types , gates, definition for sub-modules and some of displays feature related with graphical user interface.

PuNodes Module : It intended to produce PU activity patterns that match the real observed activities for Global System for Mobile Communications (GSM). We summarize general steps for PU activities that's simulate PU behavior and these steps of building Primary user units in cognitive radio network inside (puGSM.cc and puGSM.h) files within OMNET++ simulator.

PuGSM Module : It describes behaviors for each primary user using parameters and timers for attendance and absence for primary user that affected on handoff and handover state for secondary user without harmful primary user.

Proposed Primary users Behaviors Algorithm
Input/output : Primary user signals
Phase 1 : Initialize case represented by: 1- Log file recording process 2- Initializing state for application layer timer with channels(gsm1, gsm2,.. gsm20) 3- Assumption of idle/busy Duration for each PU (gsm_n): gsm1: idle Duration : 0.0300 s busy Duration :0.0500 s gsm2: idle Duration: 0.0500 s busy Duration : 0.4000 s

gsm20: idle Duration: 4.6000 s busy Duration : 5.7000 s
Phase 2 : **start Handlers functions** 1- Begin broadcasting into each connected device through data rate. 2- Indicating transmission state. 3- End of transmission PU END finish PU transmission with specific known signal. 4- Indicating finish transmission

Figure 3.9: The proposed Primary users Behaviors Algorithm.

RFSpectrum (Radio Frequency Spectrum Module): This module represented by procedures of data rate links and which setting should data rate takes to working in the proposed system .

Proposed RFSpectrum Module for Data rates links
Phase 1 : **determines whether the channel is a transmission channel by**: 1- Setting duration field of packets. 2- Setting simulation time of the sender will finish (or has finished) transmitting to find out when the channel becomes available. 3- Sum of all previous propagation delays
Phase 2 : **Process Messages** 1- Setting propagation delay 2- Setting transmission duration. 3- Check cases of the channel has lost the message. 4- Determination of data rate value.

Figure 3.10: the proposed Radio Frequency Spectrum for Data Rate Links Algorithm.

SigCommLink(signaling and communication link) : The purpose of Signaling & Communication Link (SCL) is to provide a connection among all the different

components of the CR node architecture. It does not treat data itself but it is a message-based framework implying components, gates and gate connections.

Proposed signaling & Communication Link (SCL) Module
Input/output : Overall components of CR nodes signals
Behaviors : **start Handlers functions** 1- Message checking from input spectrum sensing interface. 2- Creating objects for Control Messages 3- Collecting sensing signals and direct them to DRM module.

Figure 3.11: the proposed Signaling & Communication Link (SCL).

Distributed Resource Map (DRM) Module: It is supposed to aggregate information of the external environment and store it in a database. On the other words its collect data as signals and store them for decision making and learning as database-driven knowledge base, other components within the CR node architecture can ask for the aggregated information and use it for their own performance optimization [126].

Spectrum Sensing : This module is responsible for keeping track of the channel state and provide this information to any module requesting it. This implementation works with "crMacLayer" and provides it with request sensing results. The Figure 3.12 shows the used object link radio frequency spectrum for the data rate among CRNs node to transmit data messages.

The used RFSpectrum Module for Data rates links
- **Phase 1** : **determines whether the channel is a transmission channel by**: - Using timing technology with 20 user channels on one radio carrier. - Setting duration field of packets. - Setting simulation time of the sender will finish (or has finished) transmitting to find out when the channel becomes available. - Sum of all previous propagation delays

- **Phase 2** : **Process Messages**
- Pooling of all radio channels that are then allocated on demand to individual users.
- Setting propagation delay
- Setting transmission duration.
- Check cases of the channel has lost the message.
- Determination of data rate value.

Figure 3.12: The used Radio Frequency Spectrum Algorithm.

Core Folder : It includes message-files (Control messages, Initial, Setting, Text message objects) which are responsible for messages exchange among hierarchical of the proposed Cellular network cellphones. In addition, it contains core classes and namespaces as global parameters for functions and modules used in all simulation environment.

Images Folder: It contains on the images that are used within the layers, background and nodes, as well as changing images during execution time .

Out Folder : This folder (separate directory) contains files resulted from debugging and compiler process to build executable files in OMNET ++.

Results Folder : This folder Contains a set of files for statistical results as vector and scalar type Which can be used for analysis file (anf).

Omnetpp.ini: It contains different types of parameters can be change values during running simulation and given initial value for instance total channel, total frames and sensing duration, on the other word, to change default parameters value entered in source code file, which they will effect on the all simulation states and these parameters aren't all parameters within the used system but they are the most common used parameters.

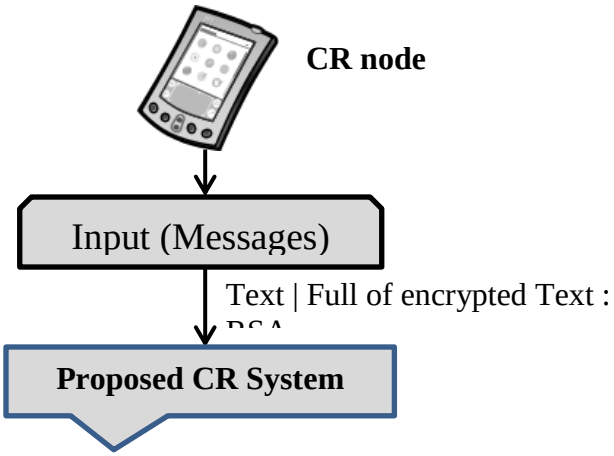
3.4 The Proposed Security System for Cognitive Radio Networks

In the first stage of simulation run time, we initialize input Keywords Messages exchanges among Cognitive Radio Units, and their equivalent encryption Cipher-Text generated from the C# programming language. Through, Secure System based RSA encryption algorithm and adapting method of FHSS. All these processes will be entered to CRNs Architecture Layers (DATA & Control Links). While, the proposed CRNs implementation in Military Application Environments.

While, each encryption value presented in (info) column within OMNET++ simulator tool at running simulation time each of these cryptography scheme has specific proposed feature for key length in RSA algorithm due to its characteristics (prime numbers, modulus, exponent) used to calculate public and private encryption key.

The RSA encryption algorithm has keyword length as plaintext length which are classified and selected from object string pool to exchange among cognitive radio units. Simulation steps represented by all processes of the proposed system through OMNET++ inside cognitive radio network with twenty channel and making recognition feature for message exchanges among nodes through data rate links and signaling & communication link (SCL).

The general steps for simulation processes can be shown in Figure 3.13, from the starting point when the input data to the cognitive radio node into building results as they represented in the following :



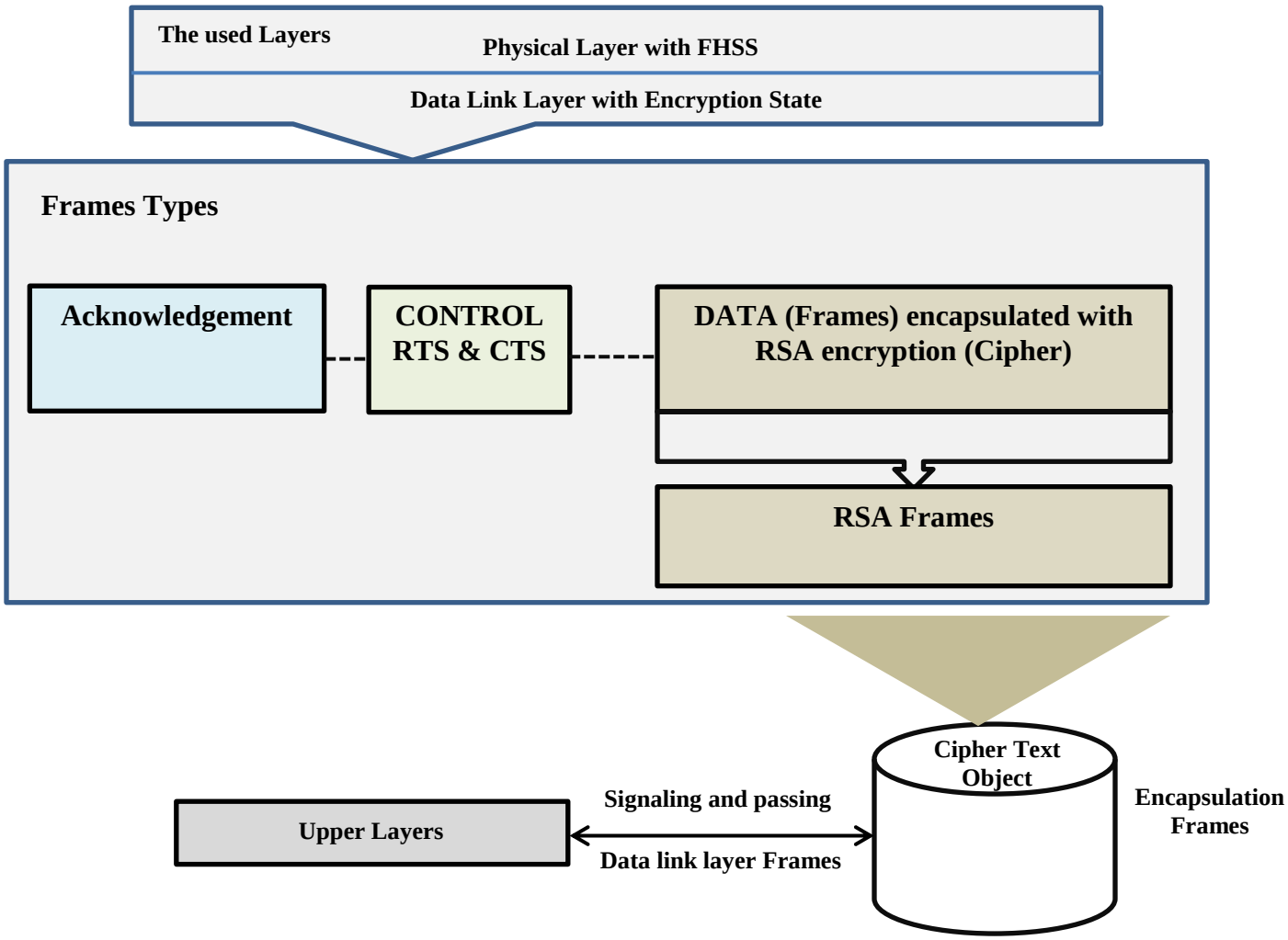


Figure 3.13: CRNs Security Scheme Block Diagram.

The message object used with the simulation environment contains the simulation parameters in the Table 3.1.

Table 3.1: Data message Object Simulation Parameters.

Message Object	**Simulation Parameters of Data messages(Frames)**
Data Message	Source

	Destination Packet-Length Proposed-Channel RTS-MAC CTS-MAC Encapsulation-modulation

While, the main used objects of GSM base station and target cognitive radio node simulation parameters as an standard features build with C++ programming language in Table 3.2.

Table 3.2 : The used of CR-Nodes Object Simulation Features

Used CR-Nodes	**Simulation features**
CR-Nodes Object	Address: Node Address Neighbors: Neighbor Node Device ID : Identifier Device Type: Cognitive Radio Node Network : CR-GSM

While the used features of GSM base station site as a Primary user station show in the Table 3.3.

Table 3.3 : The used of primary base station simulation features

The used GSM-Primary user station	**Simulation features**

GSM-Stations	ID Tx/Rx Channel : Transmit, Receive. Arrival Rate : 0.5 ms Address : Primary GSM Address Capacity : 20 GSM Primary

3.4.1 The used Cognitive radio system

In the first Section of packet, spectrum sensing in CR to determine idle proposed channel to transmission data messages and take consideration not harmful Primary user known as Global System for Mobile communication (GSM) then decide which channel free or busy. When the simulator starts, the data values for the data type are entered as keyword (message) parameters that will be considered as initial input state to the environment of the cognitive radio network. Each message type has a specific format to encapsulate their data.

The first case study with FHSS the CRNs system executed with the implementation of FHSS in Physical layer setting. The second case study with RSA the frame of the data link layer configured with encrypted text which it will encapsulated within encapsulation field and then passed to the upper layers within CRNs architecture. The third case study with the compound system configuration with RSA and FHSS each message object will configured with the based setting of the system depending on the specification for each system and all of them based on the same Frame format and these messages described below:

3.4.2 The proposed Frame Format

The header segment bits define the basic feature of the frame, and payload segment (0 - 254 bytes) contains the main data (Messages). It consists from used components below and Figure 3.14 describes them [127]:

Used channel :it represents which free channel used as idle channel to transmission messages.

Frame ID : it is designed as a slot position. The frame ID indicates the slot in which the frame should be transmitted. A frame ID is used no more than one time on each channel during one communication cycle. Each frame has a unique assigned frame ID corresponding with a unique slot. The frame ID ranges from 1 to 2047 (00000000001 to 11111111111), and the frame ID 0 is an invalid frame ID.

Data Length : it is used to indicate the size of the Encapsulation Field. encapsulation Field size is encoded in this field by setting it to the number of encapsulation data bytes divided by two (data length x 2 = number of encapsulation data bytes).

Source (Src) : it describes source MAC address .

Destination (Des) : destination MAC address

Encapsulation : it contains of security features for the used system and (Modulation Adaptation)

Data (Text Message) : it specifies input Messages entered during initial simulation state. In Figure 3.14, the used system described Frame data transmission field in cognitive radio message format.

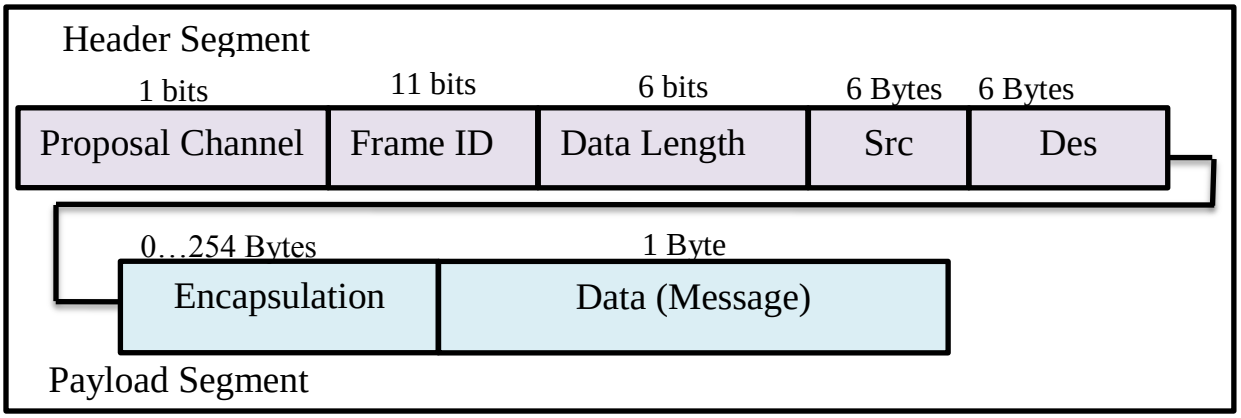


Figure 3.14 : The proposal Frame Format.

3.4.3 The proposed Control Frames

RTS (Request to Send) & CTS (Clear to Send) frames are used to enhance the virtual carrier sense process. RTS/CTS is simulated to prevent collisions from occurring.

A) RTS (Request to Send) Frame

Format of a RTS frame . It is 14 Bytes in length. Each octet represented by (8 bits). The RTS frame contains three fields, which are [128], [129]:

1. Duration : 2 octets or 2 Bytes, including the time needed for the subsequent frames in the transmit operation to be transmitted.
2. RA (Receiver Address) : 6 octets or 6 Bytes, Receiver Address indicating the MAC Address of the station that shall receive frame.
3. TA (Transmitter Address) : 6 octets or 6 Bytes, Transmitter Address indicating the MAC address of the station which has transmitted frame.

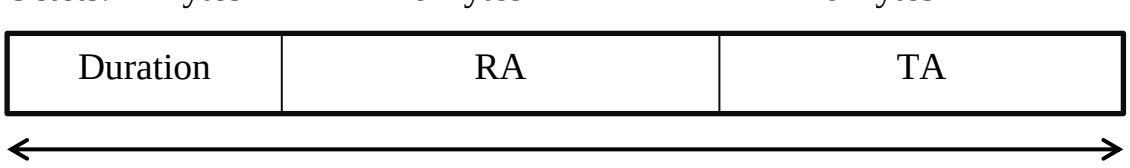


Figure 3.15: The proposed RTS Frame Format

B) 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.

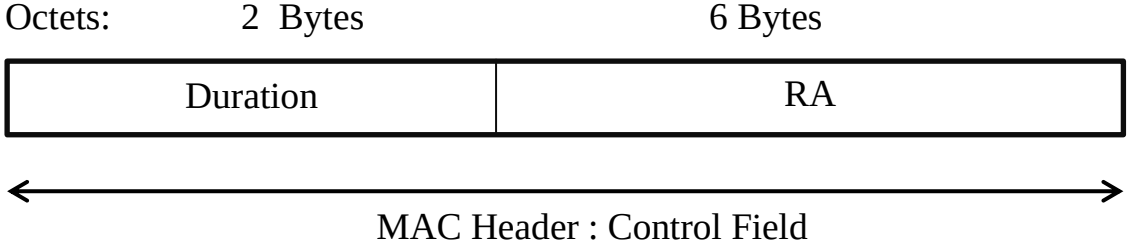


Figure 3.16: The proposed CTS Frame Format

Acknowledgement frame send to transmitter to confirming the data frame received by receiver node. As duration always set to 0. It is worth noting to the field (Duration) just within (ACK) frame. It always set to zero in order to represent the next frame request.

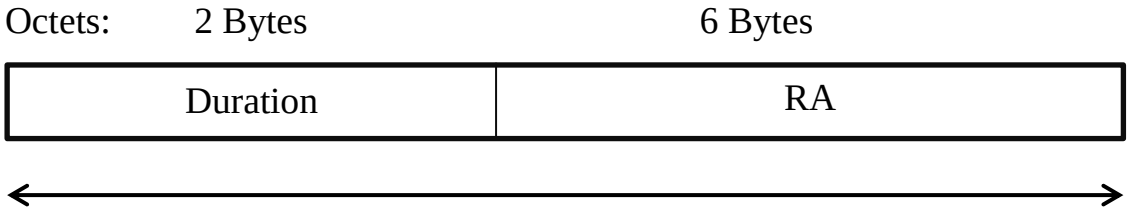


Figure 3.17: The proposed Acknowledgement Frame Format

3.5 The proposed Noise-Jamming Attack System

We simulate the noise-jamming attack case as the physical layer security attack, which it effects on the transmission medium, the proposed system mitigate the noise attack with spread spectrum technique as the FHSSS, the noise attack by retransmission through different channels or through a large bandwidth or large number of channels .The physical layer considered the most damage layer from the radio noise-jamming attacks.

The main effect of the jamming(noise attack) is reducing network traffic by effecting on the network performance with disrupt network function, the jammer attack use the link-noise attack by building list of link-noise attacker packets as a fake packet which are injected to the sorted packets of the source packet node and then sent to the destination link communication.

The Figure 3.18 and Figure 3.19 showed the link-noise attackers how it effects on the link of the source packet and which it passed to the destination link, when packet sent from source to destination, it added to the destination queue based on the arrival time, the attacker modified probability of loss packets by

modified the original link probability and the additional noise produced by the attacker. Besides,

If a Fake packet injector attacker has to be simulated, new packets have to be injected into the transmission queue once the packet is inserted in this queue, the network transmits these fake packets as if they were genuine.

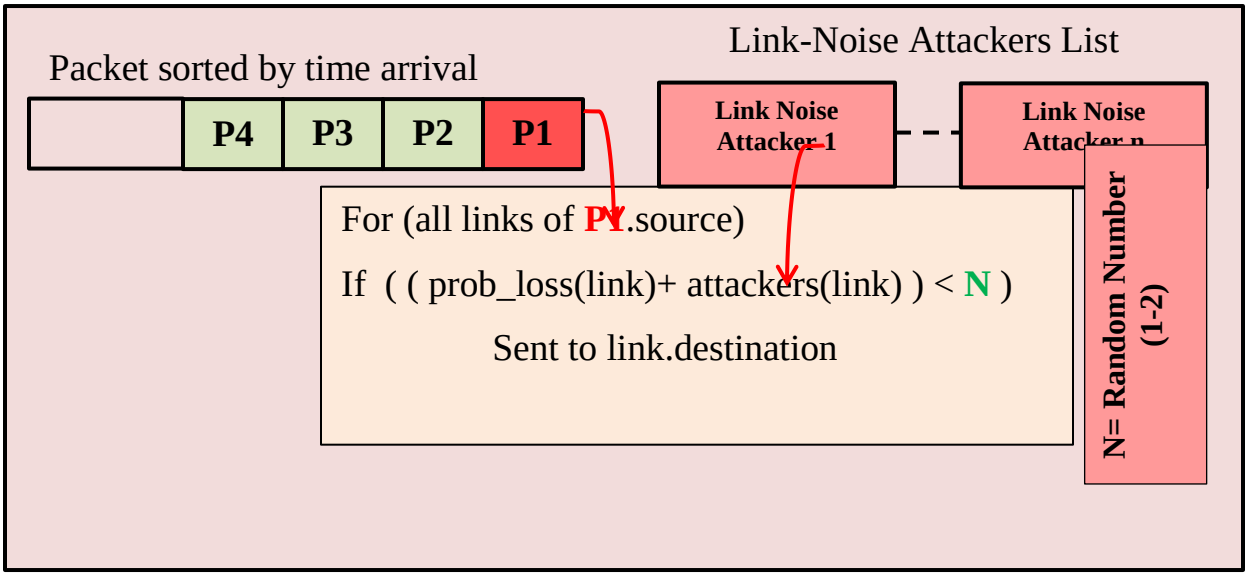
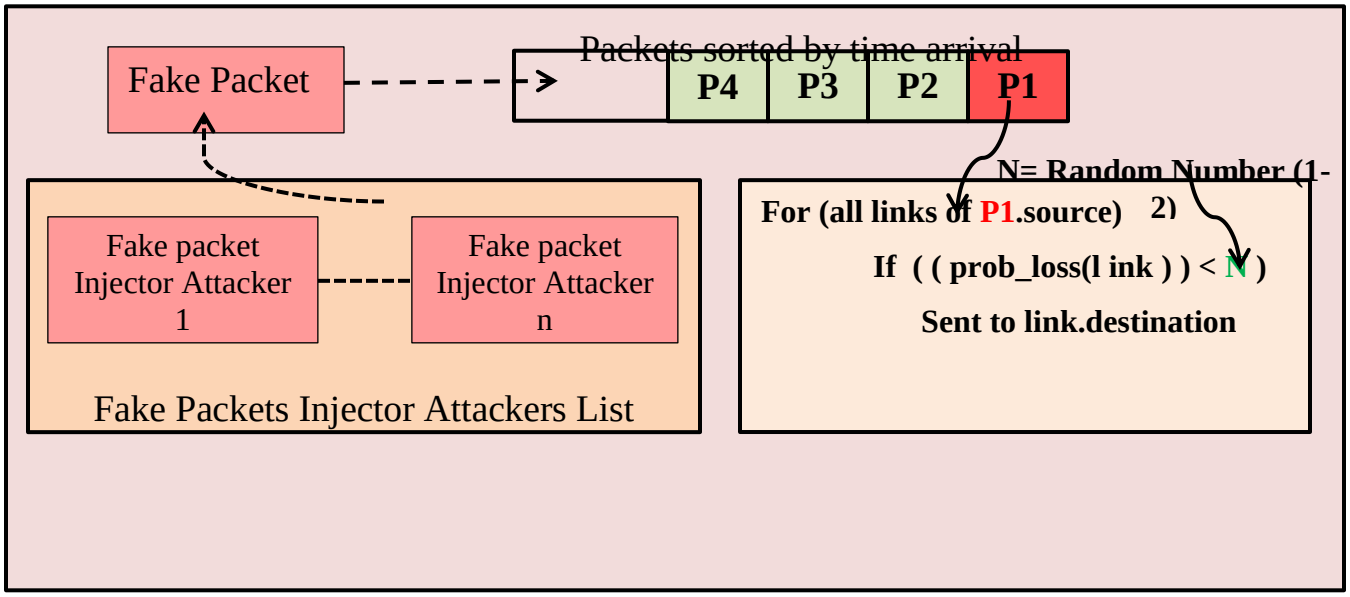


Figure 13.18 : Link-Noise Attackers List.



Of course, during the implementation of the proposed work, we faced several determinants in a simulation environment. However, we summarize these existing challenges as follows:

3.6.1 Mobility

The proposed work does not support mobility of nodes in contrast data rate spectrum fixed link. There is a different reason, for instance, complexity in routing packet where channel dynamics are very high even for static scenarios on other hands mobility required movement nodes from one connection to another within another coverage area based on mobility pattern. in addition, handover protocol channels are simpler in fixed cases and all nodes can follow a similar approach to connecting with a cognitive radio network.

Generally, There are specific extensions introduced by the open source developers to support node mobility feature, for example, using "MiXiM" model into our CR simulation environment. The MiXiM is an OMNeT++ modeling framework created for mobile and fixed wireless networks (wireless sensor networks, body area networks, ad-hoc networks, vehicular networks, and so on). It offers detailed models of radio wave propagation, interference estimation, radio transceiver power consumption and wireless MAC protocols for example, Zigbee.

3.6.2 Free Secure library

The lack of security libraries is one of the most challenge of designing a network security system. This is the result of different releases of the simulator tools and library compatibility with modern versions and the ability to implement cryptographic algorithms and security protocols at the same time. so it's considered time consumed especially researchers restricted by time. On the other hand, there is crypto++ library in "OMNET++" with some security model but as we explained previously need more attention and developing.

3.6.3 Implementation Time

It explained by the time to implement and to design simulation environment with simulation tools (OMNET++, C# programming language, and workbench) within the practical side and the time to get information about the proposed system within the theoretical side. In addition, the lack of prior experience to achieve the proposed system features.

The implementation of the proposed system was based on a programmatic method that relied on a set of tools that were clarified above. Besides, Most of the components of nodes and the related schemes were applied within the simulation network state. The libraries that provide support in implementing the proposed system were of the cognitive radio network represented by the open-source library as (Cognitive Radio library) and libraries for Frequency-hopping spread spectrum (FHSS) , which is represented by (Ieee80211FHSSMode) library. Both libraries are based on the programming language C ++. Where the main library contained the architecture, the communication layers, interconnection layers as well as the classes of some of its hardware components in programmable way of the proposed network , the fourth chapter will deal with how to implement the proposed network within this environment in practical simulation way.

CHAPTER FOUR

Simulation, Results and Discussion

4.1 Introduction

This chapter provides the simulation and discussion of results for the proposed security system, that presented in chapter three. It has simulated by using OMNET++ and c# programming language to implemented the encryption and decryption processes in the proposed system.

Enhancement the security of the cognitive radio network during this thesis is done through the use of RSA cryptography algorithm. As well as, spread spectrum technique represented by Frequency Hopping Spread Spectrum (FHSS) to enhancing throughput and data rate transmission. The keywords (messages) entered into the network as specific sentence within the military application words, where they are entered as an data objects and they encrypted using outside library in C # to get the encrypted text then insert it into the implementation interface to be exchanged among cognitive nodes in the network.

The proposed security system implemented by three cases studies where the first one with the security system based on the RSA implementation in Omnet++ with C#, the second one with spreading technique as FHSS , while the last case study with compound approach based on RSA and FHSS case. Each of these cases study contains the same parameters that evaluate our proposed system as well as prove the enhancing in the security of the Cognitive Radio Network .

It has been presented the results as follows:

1- Calculating Throughput, Data Drop Rate, and Detection Time simulation parameters for each case study.
2- Calculating the data signals (Frames) that arrived without error to the receiver on each reception node.
3- Evaluating the quality of the proposed system by using message statistic tests which determine how many message scheduled through overall simulation time for all cognitive radio network nodes.

4- Calculating the number of control messages exchange among transmitters and receivers.
5- Calculating the number of negative acknowledgments which are given indication about not arrived message and require to resend.
6- Calculating the number of hand over from a specific case which is effected on the acquisition of the mutual channel between PU and SU.

The proposed simulation parameters setting for all case studies (entire proposed system in OMNET++ simulator) as shown in Table 4.1.

Table 4.1: Simulation Parameters Setting.

Parameters	**Value**
Simulation Time	30 minutes
Total Frames	1024 frames
Sensing interval	0.05 ms
Proposed Channel	20 channels
PU Arrival Rate	Variable 0.5-1s
PU Tx Duration	0.5s
Number of nodes	6 SUs , 20 PUs
MAC Layer	802.11b standard
Data Type	String Message

The proposed system is implemented with these simulation and programming language tools. Where more than one tool has been adopted to implement the proposed system, and each of them has a specific goal for implementation purposes, as shown in the Table 4.2.

Table 4.2: The Proposed Tools.

Tools	**Installation Requirements**	**Goal of using the tool**
Omnet++ 4.6	Windows 7 (32-bit or 64-bit) -1 1 GB (32-bit) or 2 GB (64-bit) RAM -2	Simulating the proposed CRNs in military network with GSM sites.

Microsoft Visual studio 2010	Windows 7 (32-bit or 64-bit) -1 Microsoft .NET Framework 4.0 -2 1 GB (32-bit) or 2 GB (64-bit) RAM -3	Implementing RSA algorithm to encrypt messages exchanging among cognitive radio nodes

4.2 Case studies of proposed Secure Cognitive Radio Network system

The used system describes an enhanced secure Cognitive Radio system in OMNET++. All of the used CRNs elements in the proposed regions contain 6 secondary users nodes and 20 Mobile communication (GSM) base station as Primary users as shown in Table 4.3.

Table 4.3: The used CRNs Elements.

CRN Elements			
SUs Transmitter Nodes	battalion	corps	fieldtraining
SUs Receiver Nodes	infantryforces	combatteam	coveringposition
GSMs	gsm,gsm1,gsm2,……..gsm19		

The results of the proposed system based on many statistical models inspired in OMNET++ simulator as follows:

- Count: number of signals as sensing or frames,
- Max : maximum number for signals.
- Min: minimum number of signals.
- Mean: is the average and is computed as the sum of all the observed outcomes from the sample divided by the total number of events.
- sqrsum: Square of summation.
- stddev: the standard deviation is a measure that is used to quantify the amount of variation or dispersion of a set of data values.

The Figure 4.1, shows the general CRNs network topology with the main network elements.

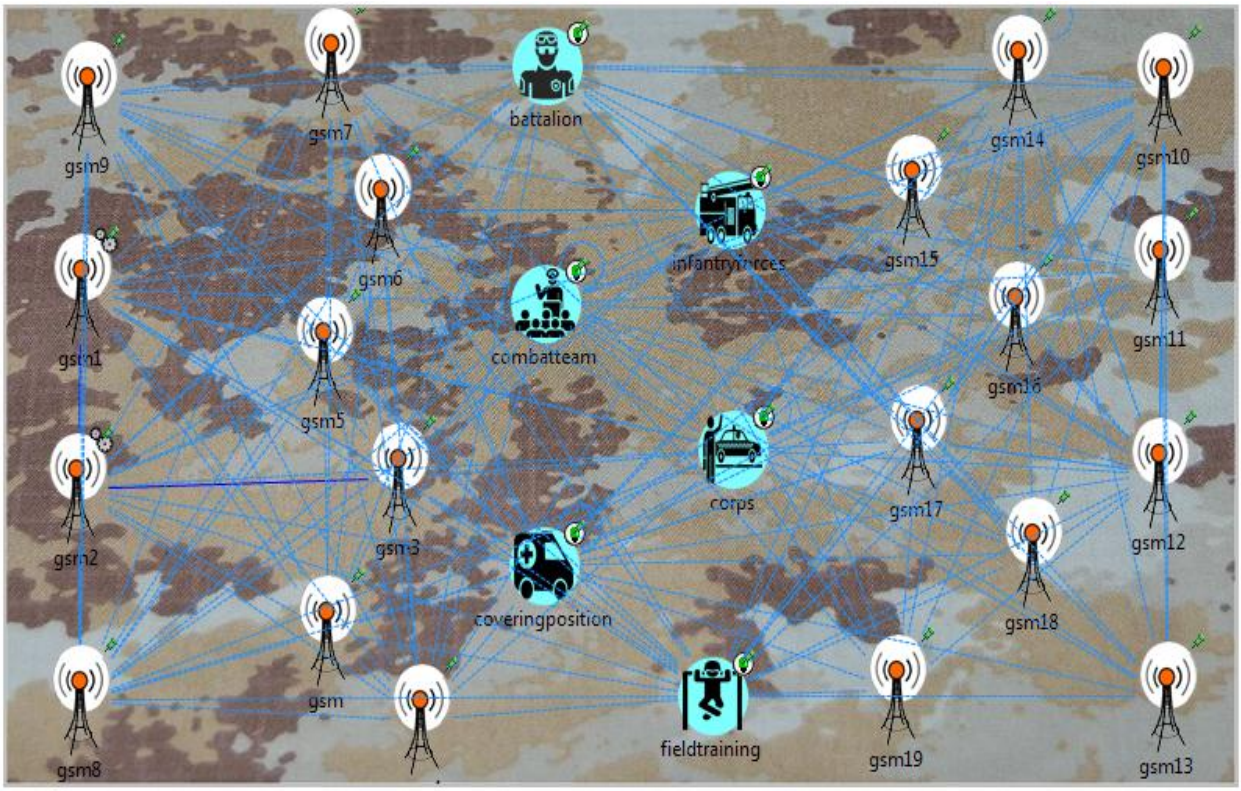


Figure 4.1: The proposed Topology of CRNs in Military Application.

There are many variables that have been taken into consideration when comparing the three study cases which recognize and proved our proposed system will be better compared with other study cases for example :

1- Determining Data Drop rate

2- How much Detection Time to sense and getting idle channel?

3- How many active nodes found in the entire network ?

4- How many scheduled messages during the simulation time ?

5- How many data link layer frames arrived without errors?

6- How many Negative acknowledgment through transmission period?

7- How many maximum throughput values for data transmission through the transmission time?

Determining the number of active nodes in the network is one of the most important criteria for the network performance measurement. The shorter period to complete the building of addresses, routing directions and the communication between nodes refer that better network performance due to the network requires less computation power to build the network statistics.

During simulation state of the proposed system there are some of fields objects and classes contain on the base objects entity as class name, details, class owner, default list, Gates and the main simulation parameters. While the Contents represent the used values of total channels, Primary Users and Secondary Users objects and their properties such as Name and Information field.

The Figure 4.2, and Figure 4.3, show some of the main simulation parameters objects (fields and contents) which are implemented and executed within the used simulator (OMNET++ 4.6 release) .

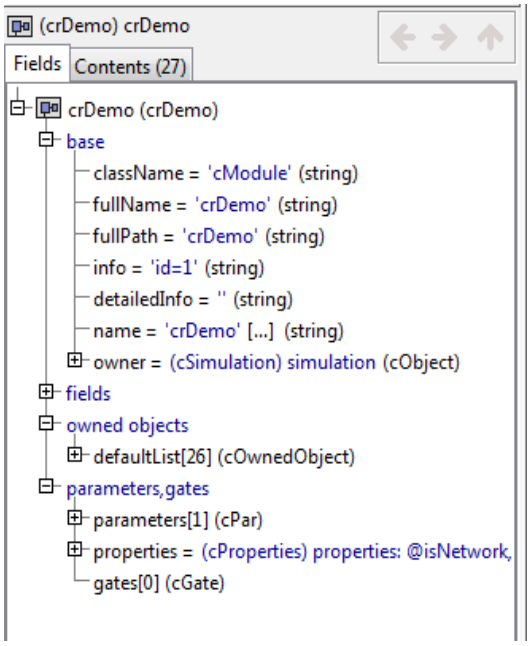


Figure 4.2:The used CRNs Object Fields.

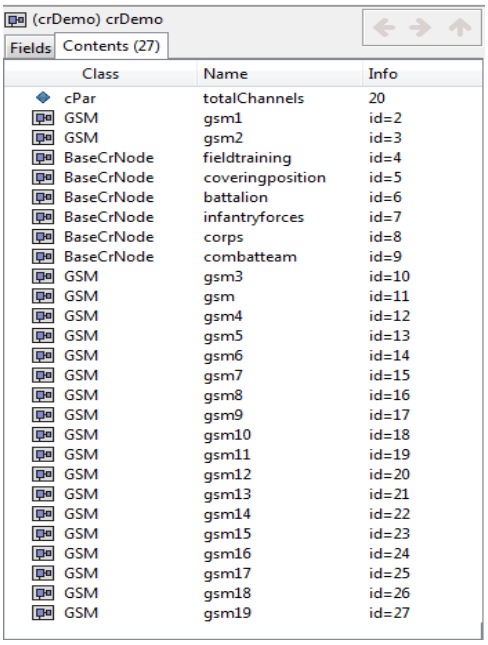


Figure 4.3: The used Contents in OMNET++.

The role of the proposed countermeasures is to make a CRNs immune to Noise-Jamming attacks rather than reactively respond to such incidents attack. The best results simulated with encryption of packets based on the RSA and

Frequency Hoppy Spread Spectrum (FHSS) transmission in parallel case (FHSS and RSA case study). The RSA provides encryption of link-layer packets to ensure a high entry barrier for Noise-Jamming attack, While FHSS, it minimizes unauthorized interception and jamming of radio transmission between the nodes. Noise attack effects by decreased Throughput , increased data drop rate, detection Time and delay Time, so It can easily disrupt a network.

The proposed Noise-Jamming attack happened between Secondary users by adding fake packets (fake messages) to the transmission data packets and in some cases it occurs between Primary user and Secondary user by effecting on the spectrum sensing by false alarm notifications and which effected on the detection idle channel among proposed channel within the system. The Figure 4.4, and Figure 4.5, Showed the Noise- Jammer attack in CRNs between Secondary users and between Primary user and Secondary User.

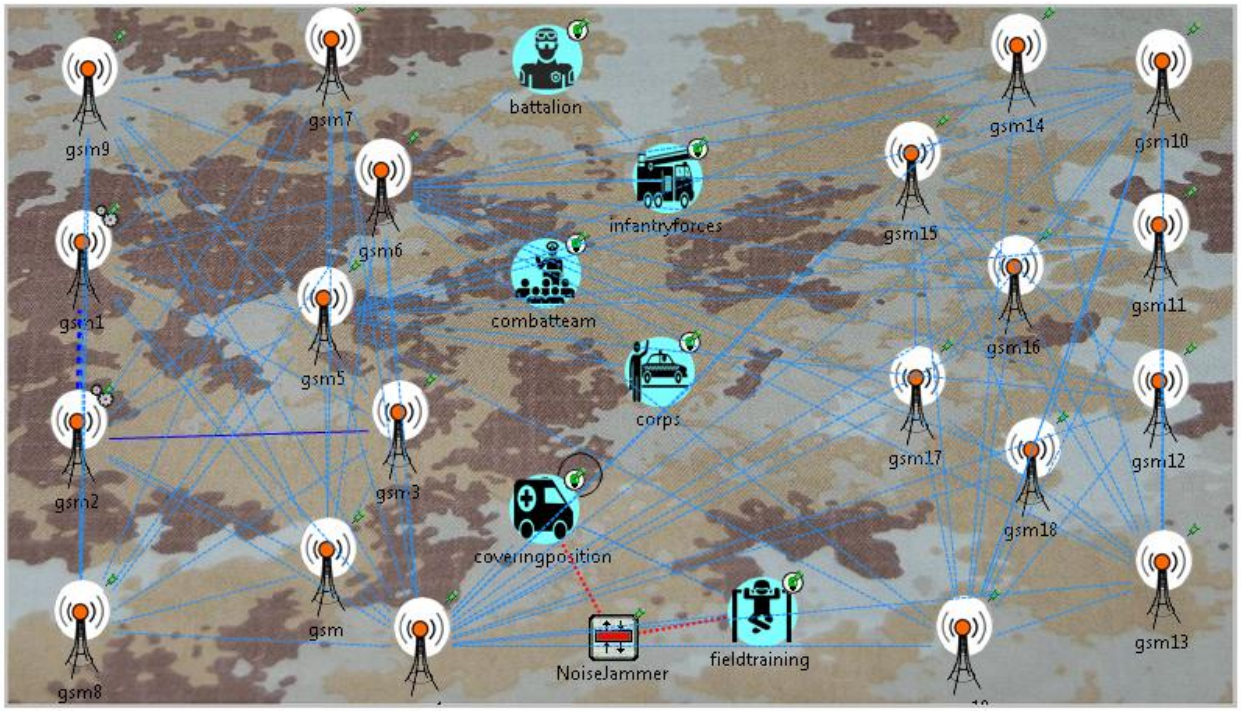


Figure 4.4: Noise-jammer attack between Secondary Users of CRNs.

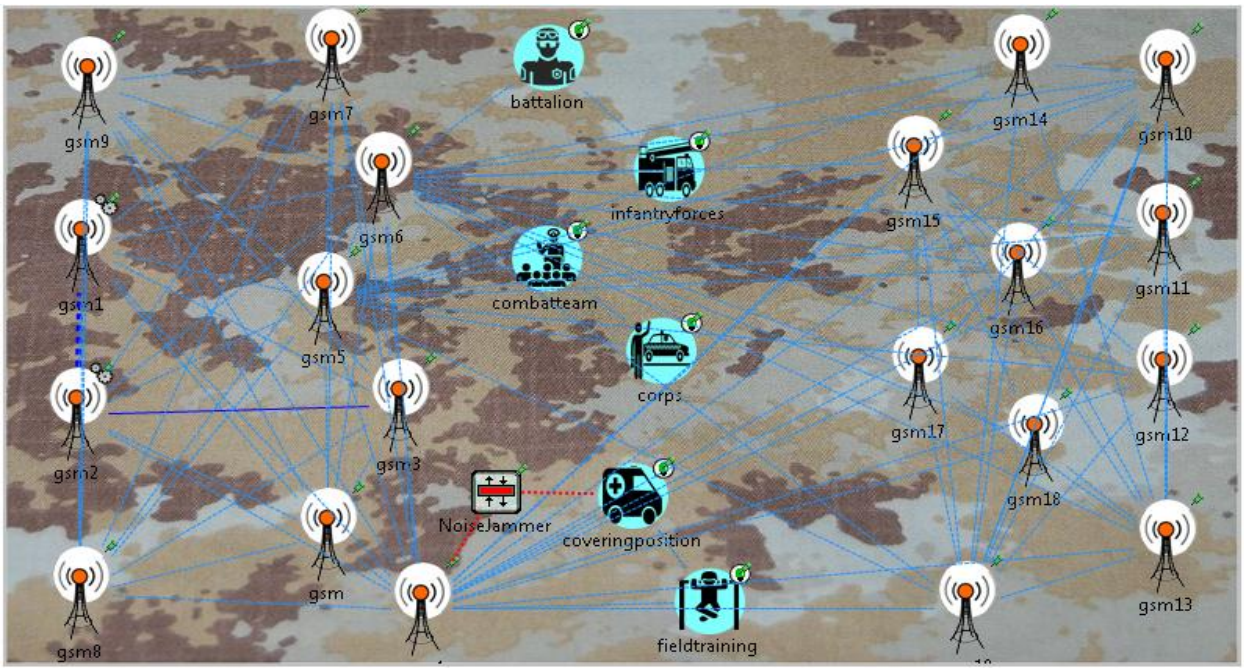


Figure 4.5: Noise-jammer attack between Primary and Secondary Users of CRNs.

4.2.1 Case study of proposed FHSS of Cognitive Radio Network

The first case study with frequency hopping explained in the Figure 4.6, to messages exchanged between transmitter and receiver and how they are passing through frequency bands with twenty proposed channels (1,…,20).As mentioned, there are parameters should taking into consideration through designing any system within plaining stage, and these parameters are number of nodes in the networks, and data type which will be transmitting through the network.

So, the used system built with simulation case as explained and also possible to take this advantage to build other developmental models in the future for practical implementation, especially in networks where the power factor is very important, especially the cognitive radio network sensor applications inspired in military applications.

We will illustrate many parameters within the statistical results that will be passed signals between layers and for each transmitter nodes and receiver nodes under Layers. These parameters implemented in the main layers that contain

algorithms for the proposed system. As well as, they are affected from one node to the another one of each case study.

The Figure 4.6, showed some of statistics results for (application layer request which are help to get the channel from primary user, the control information request represent by RTS control message in MAC layer, sensing a signal to make the appropriate decision in the spectrum sensor module).

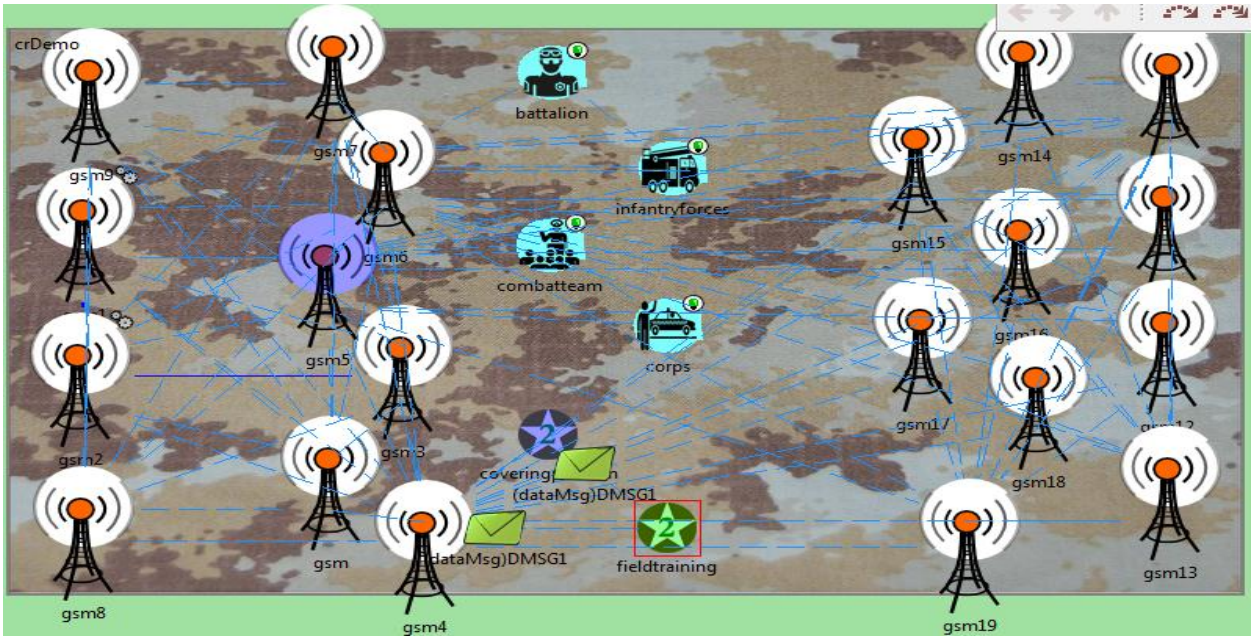


Figure 4.6 : Messages objects exchanges of CRNs in OMNET++.

The Table 4.4, summarizes the results for proposed layer from all transmitter nodes as (battalion, corps and fieldtraining) with theses parameters in application Layer as (appRequest : application layer request for signaling to show within graphical user interface values) and within MAC Layer (rtsFailSignal : Request to send fail signals), (rtsSignal:Request to send signals secsseful arrived), handover : system take the channel for transmission), and within spectrum sensing of physical layer as (sensing signal: number of sensing signals within physical layer of Cognitive radio nodes) .

Table 4.4: Application Layer request, Mac Layer and Spectrum Sensing Values within FHSS Case Study.

Application Layer		MAC Layer		Spectrum Sensing	
appRequest	**0-44**	rtsFailSignal	**0**	sensingSignal	**10-54**
		rtsSignal	**6-50**		
		handover	**0-1**		

The Figure 4.7, shows the Application Layer request, Mac Layer and Spectrum Sensing Values from all transmitter nodes explained above (three transmitter nodes : battalion, corps, fieldtraining).

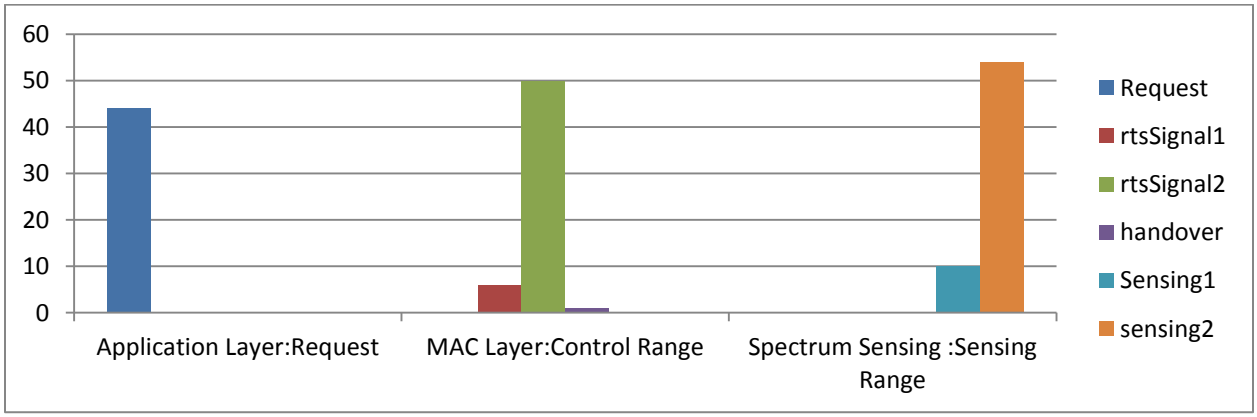


Figure 4.7: Application Layer request, Mac Layer and Spectrum Sensing Values from the Transmitter Nodes within FHSS Case Study .

Table 4.5, summarizes the results rate for data and sensing signals according the proposed modules from all Receiver nodes as (infantryforces, combatteam and coveringposition) and the simulation parameters as (MAC Layer NACKs : Nagative Acknowldegments signals for the messages which have errors or lost messages as control messages within data link layer objects, spectrum sensing : spectrum sensing signals for spectrum sensing information within Physical layer).

Table 4.5: Negative Acknowledgments Signals and Spectrum Sensing all Receiver Nodes within FHSS Case Study.

MAC Layer NACKs		Spectrum Sensing	
NACKsSignal	**0-2**	sensingSignal	**21-65**

While, Figure 4.8, shows the Nagative Acknowldegments signals and Spectrum Sensing all Receiver Nodes (infantryforces, combatteam and coveringposition).

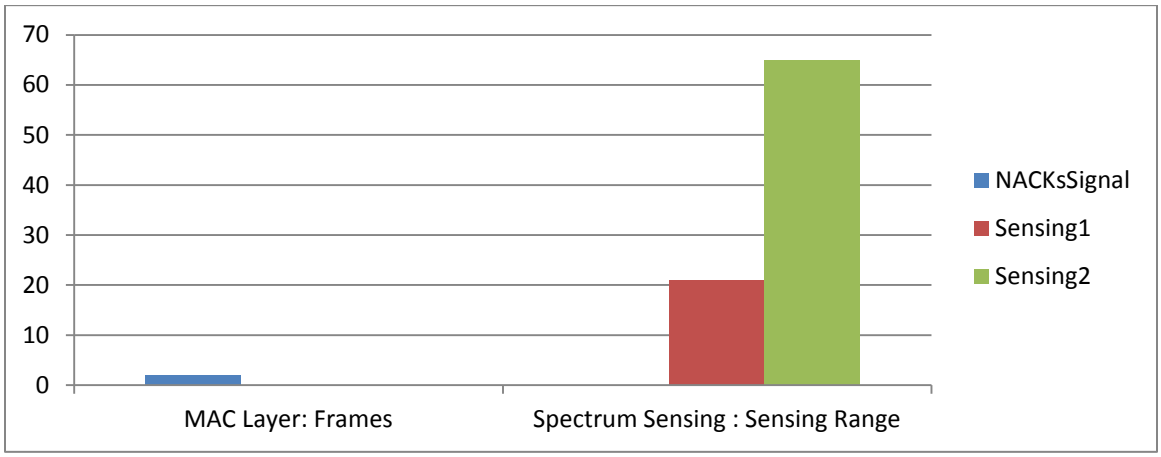


Figure 4.8: MAC Layer NACKs and Spectrum Sensing from Receivers Nodes within FHSS Case Study .

The Table 4.6, showed the number of transmission and reception data frames messages from the transmitters / receivers nodes, and summation values for data message created in all nodes .

Table 4.6 : Sent and Received Data Messages for the FHSS Case Study.

CR Transmitter nodes	**Sent Data messages**	**Sum**	**CR Receiver nodes**	**Received Data messages**	**Sum**
corps	460	1162	combatteam	393	1056
battalion	365		infantryforces	340	
fieldtraining	337		coveringposition	323	

While Table 4.7 and Figure 4.9 explained the main simulation parameters used for comparison with all case studies and this table for the first case study of FHSS implementation.

Table 4.7 : Main simulation parameters for the FHSS Case Study.

Throughput in Mbps	Data Drop Rate in Mbps	Detection Time in Seconds	Delay Time in Seconds
0.908	0.091	0.416	0.275

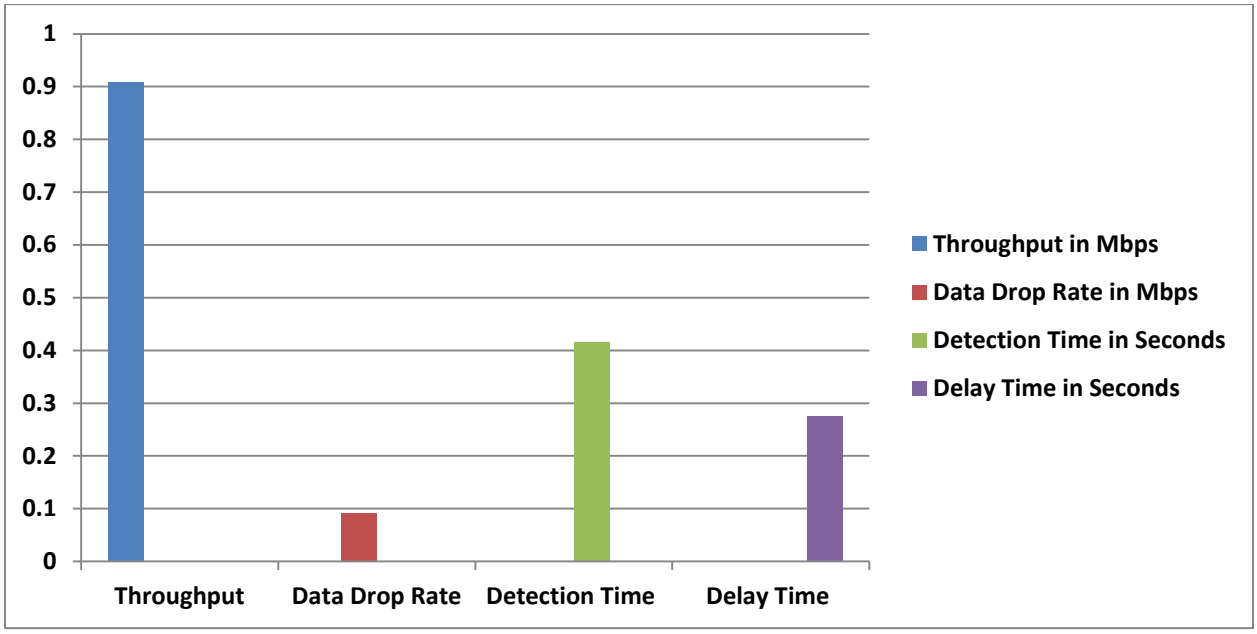


Figure 4.9: Throughput, Data Drop Rate, Detection Time and Delay Time for FHSS Case Study.

This case for the proposed FHSS system gives us the best results compared with other cases because there is a maximum data rate as throughput passed through entire network transmission and the summation of all messages arrived without errors are (1162). After completion of the implementation of the proposed system, we recorded the events for different system procedures represented by processes(sensing, decision-making) and messages (Acknowldgement, Control, DATA) exchanged among the military application nodes through entire the network.

The Figure 4.10, illustrates the log file states for each type of messages from all elements in the network . The log file configureed with theses feaures as :

- X-represents arrival time for each component in the network
- Y- represents the component objects (Pus and Sus)
- Nonlinear timeline setting mode
- Axis ordering mode
- Showing / hiding
    - Message sending
    - Message reuse : showing retransmitted messaged
    - Dependencies
    - Self message transmissions

      showing self-message again for next transmission required for next message or retransmitted loosed or timer out messages.
    - Method calls
    - Transmission duration information
    - The number of events
    - The name of messages

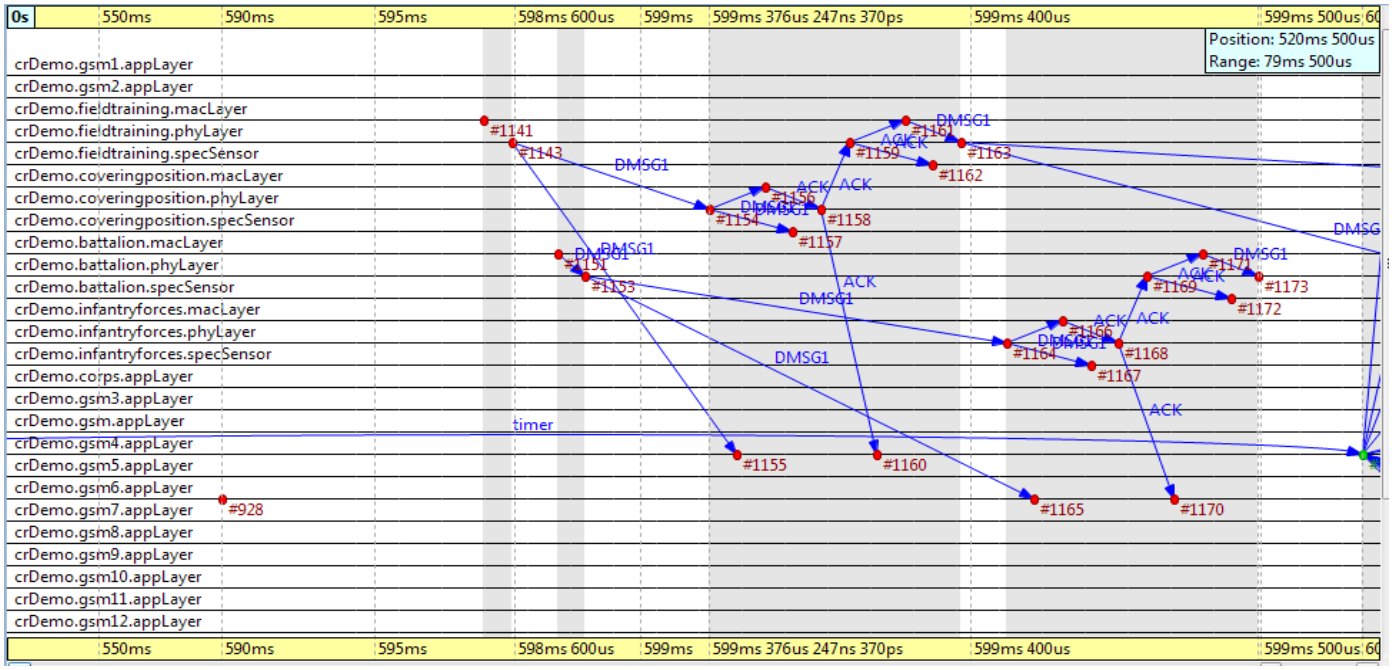


Figure 4.10: Behaviors of the proposed FHSS Case in Log File .

While the Noise attack of the FHSS case study with the main simulation parameters showed within the Table 4.8 and the Figure 4.11.

Table 4.8 : Main simulation parameters for Noise-Jamming Attack within the FHSS Case Study.

Throughput in Mbps	Data Drop Rate in Mbps	Detection Time in Seconds	Delay Time in Seconds
0.844	0.097	0.445	0.294

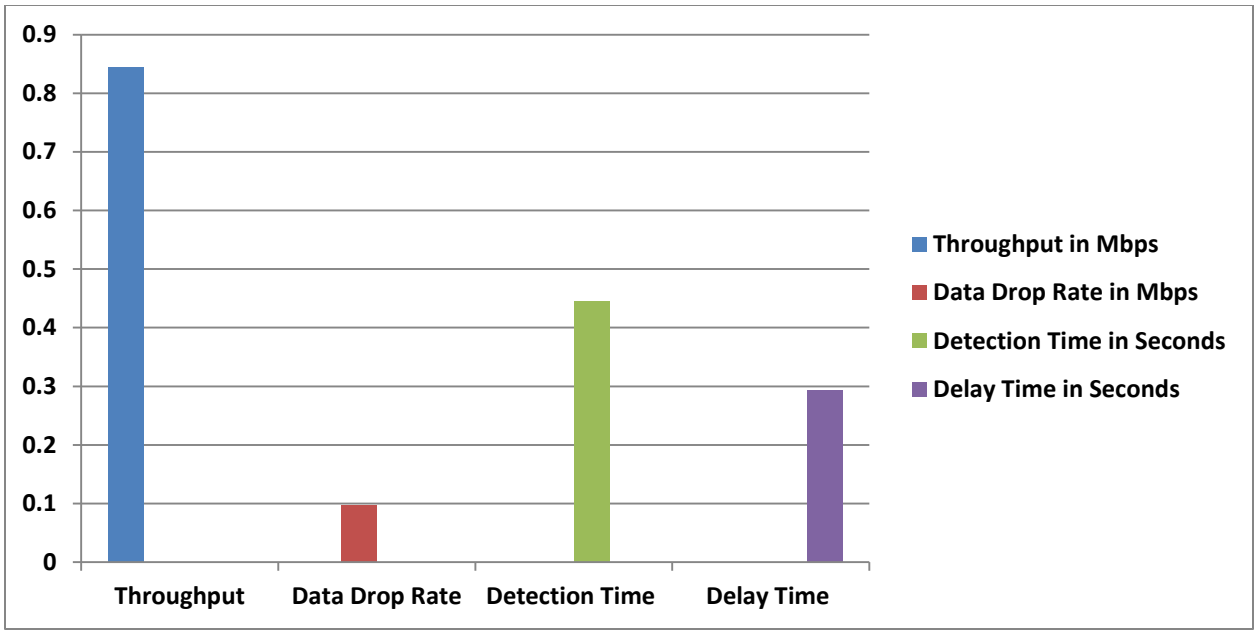


Figure 4.11: Throughput, Data Drop Rate, Detection Time and Delay Time of Noise-Jamming Attack within for FHSS Case Study.

4.2.2 Case study of the RSA security of Cognitive Radio Network

The cognitive radio network with a security system based on the RSA security algorithm. This network was built to simulate the network requirements of the cognitive node within the simulator OMNET ++ and security features added with Visual studio C#. The used method encrypted input message through the specific interface through execution the system and then value will passed to the system and then to the particular section within the frame which it determined to encryption field which is exchanged among cognitive radio nodes as encryption messaged not clear to the unauthorized users.

Behavior of the network attackers for example (malicious, selfish, misbehave, etc.) leave adverse effect on the performance of the network. On the other hand, there are many security requirements should investigate the network to ensure communication security, so many security models proposed in recent years to resolve the security issues for such behaviors. In general, most of these models have focused on the importance of security, regardless of the other things such as

energy or the complexity of the design model, especially matters related to the limitations of the sensors

Each cognitive radio node consists of five layers of communication model represented by (application layer, transport, network, MAC and physical) layers. Where different messages are transmitted through these layers and then building statistics based on simulation parameters. So the networks' elements are Base Station(PU) with application layer which is send a query when PU attends or leaves from the channel within the specified periods determine through PU arrival duration.

The result of implementing this topology within the same simulation time about (30 minutes) given (6) active node through the entire network as well as more than 300 scheduled message objects runtime queue.

During the data entry stage, in this study case, the encrypted data that was generated with C # as follows, where the following text is entered in encrypted form for instance in Table 4.8:

Table 4.9: Plain-text and Cipher Text Sample.

Plain-Text	go ahead
Cipher-Text with RSA	2CzqqJKxfu4xEq1GV9Jm2u7rmsCe65wKzPTw5jtS38n2tVEGio

While, the Figure 4.12, explained the used RSA method to encrypt plain-text which will be pass to the cognitive radio system and the used Form created with C# code beind and implemented with Microsoft Visual studio 2010.

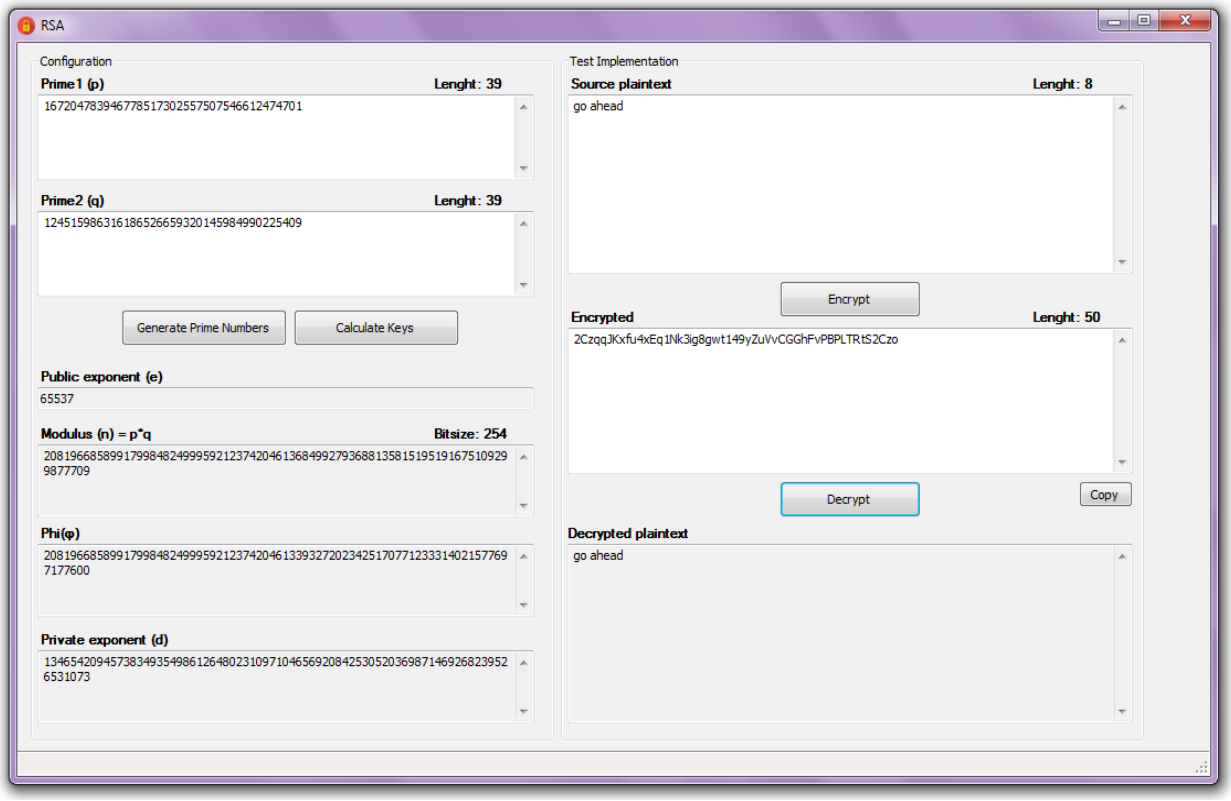


Figure 4.12: The used RSA Method.

Within Figure 4.12, contains on different methods showed in the Table 4.10:

Table 4.10 : RSA Methods and Description.

RSA Methods	Description
Generate Primes Number	- Generating Primary numbers based on (p) and (q) values which they generated dynamically by the system method. - Determining Bit Size Based on Prime1(p) and Prime 2 (q).
Calculating Keys	- Calculating Keys with: - Using Public Exponent (e) generated by system method. - Finding the value of Modulus (n)=p*q

	Building Phi(φ) - Creating Private Exponent (d) -
Encrypt	Call Encrypt process to encrypt plaint-text. - Verify Key length if Key too small return to generate and to calculate new key. - Dividing plain text to block. - Add padding based on the random generator, and make sure the first bit is always zero. No negative numbers for (d). - Generating Cipher text. -
Decrypt	Call Decrypt process with: - Initializing cipher text value. - Creating Arrays for decoding values in Hexadecimal characters. - Remove padding. - Decrypt arrays. -

As this parameter is passed to the OMNET++ system and from there to the part of encapsulating field within the data field to be sent later, and it is transmitted among the CR nodes within the network system, which represented in encrypted form and unclear to preserve the sent data as shown in the Figure 4.13.

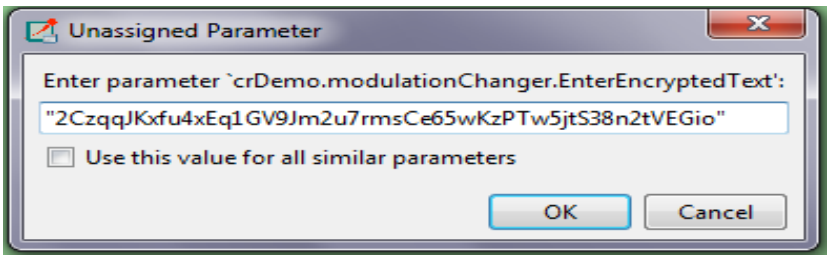


Figure 4.13: The encrypted Form with OMNET++.

The Table 4.11, and Figure 4.14, summarizes the signals values for application layer , mac layer and spectrum sensing from all transmitter nodes as (battalion, corps and fieldtraining) with the (Application layer request : appRequest, Request to send signal : rtsFailSignal- rtsSignal, Handover to get spectrum channel acquisition and spectrum sensing features with sensingSignal parameter).

Table 4.11: Application Layer request, Mac Layer and Spectrum Sensing Values from all Transmitter Nodes within RSA Case Study.

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**0-35**	rtsFailSignal	**0**	sensingSignal	**10-44**
		rtsSignal	**6-41**		
		handover	**0-2**		

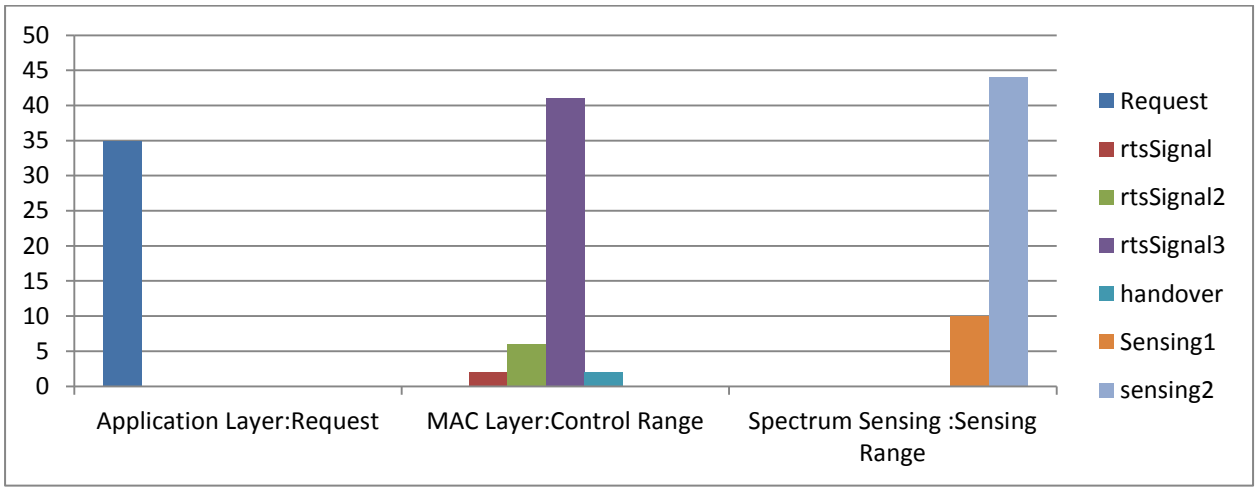


Figure 4.14: Application Layer request, Mac Layer and Spectrum Sensing Values from all Transmitter Nodes within RSA Case Study.

The Table 4.12, summarizes the results for the data and sensing signals from all Receiver nodes as (infantryforces, combatteam and coveringposition)

Table 4.12: MAC Layer Negative Acknowledgements and Spectrum Sensing values from all Receiver Nodes within RSA Case study.

MAC Layer NACKs	**Spectrum Sensing**

NACKsSignal	**0-6**	sensingSignal	**20-43**

While, the Figure 4.15, shows results statics for all receiver nodes as (infantryforces, combatteam and coveringposition).

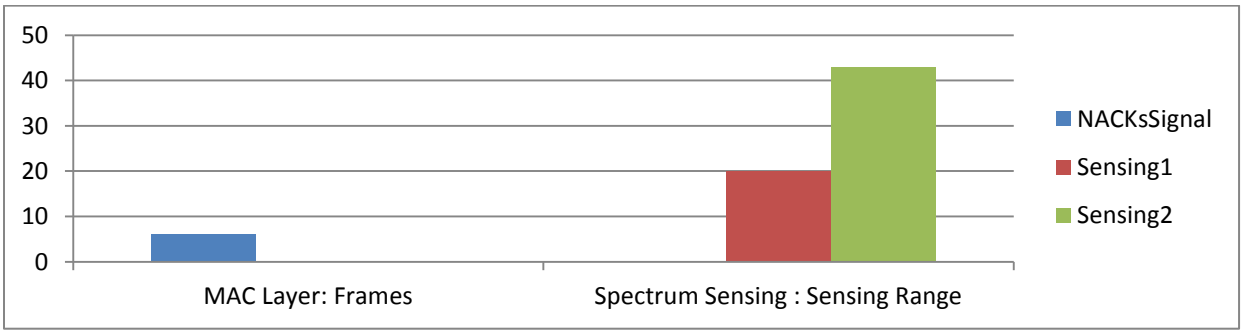


Figure 4.15: MAC Layer NACKs and Spectrum Sensing from all Receivers Nodes within RSA Case study.

The Table 4.13, showed the number of transmission and reception data frames messages in the RSA case study.

Table 4.13 : Sent and Received Data Messages for the RSA Case Study.

CR Transmitter nodes	**Sent Data messages**	**Sum**	**CR Receiver nodes**	**Received Data messages**	**Sum**
battalion	352	758	infantryforces	282	513
corps	278		combatteam	147	
fieldtraining	128		coveringposition	84	

While Table 4.14 and Figure 4.16, explained the main simulation parameters used for comparison with all case studies and this table for the second case study of RSA implementation based on the simulation values generated in Table 4.13 above, which it contains all simulation values from transmitter and receiver nodes.

Table 4.14 : Main Simulation Parameters for the RSA Case Study.

Throughput in Mbps	Data Drop Rate in Mbps	Detection Time in Seconds	Delay Time in Seconds
0.676	0.323	1.333	0.369

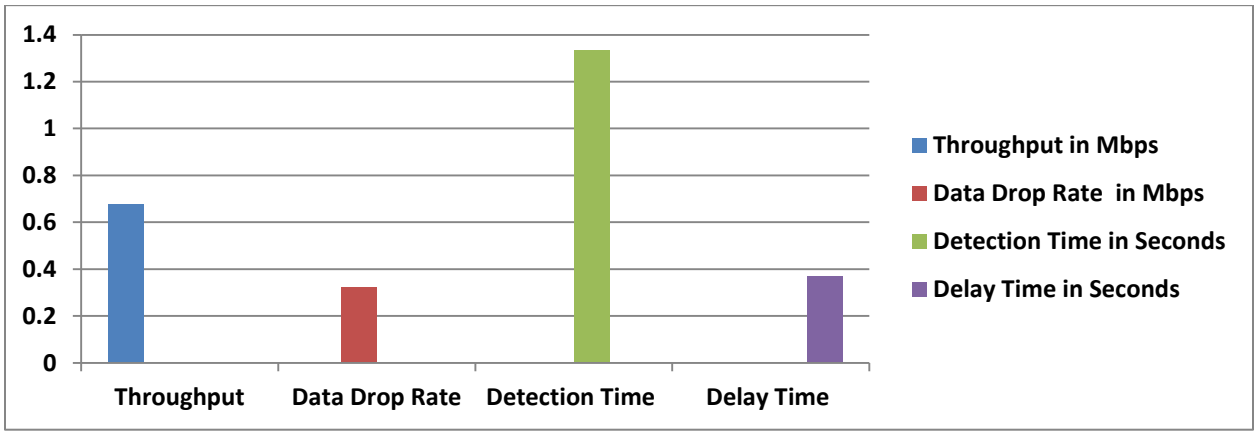


Figure 4.16: Throughput, Data Drop Rate, Detection Time and Delay Time for RSA Case Study.

Within the event recording process for this case study through general.elog file or event log file.The final form of behaviors for each node within the network was illustrated through cognitive radio elements (secondary users and primary users). Where we observe the random behavior of some nodes as well as they trying to exploit the channel and change schedules of neighboring nodes.

We used different parameters to describe this study case within statistical results for statistics module that's concerning to all nodes in the network. Here we can see how this behavior is slow for some nodes as well as how the irregular transmission occurs. Where the channel is exploited from some nodes for a longer period than others and in a repetitive and transitional, looping way through the allocated periods to transfer data from another node.if we compare this case with the proposed system and how the impact of the data transferred to the entire life cycle of the cognitive radio node. We will see that system does not have a malicious behavior but it has a slow and not secure state. Furthermore, some of the problems related to the spectrum sensing and decision-making by the contract

exploited channel.The Figure 4.14, iullstrated the general behaviour for cofnitive radio network with security requirements and mechanisum to support cognitive radio netwrok behaviour and cognitive radio cycle . The log file showed different messages status types (PuBusy, PuEnd, RTS, CTS, ACK, DATA) and ack-time out as well as, all sensing signals for instance (app-request,app-timer).

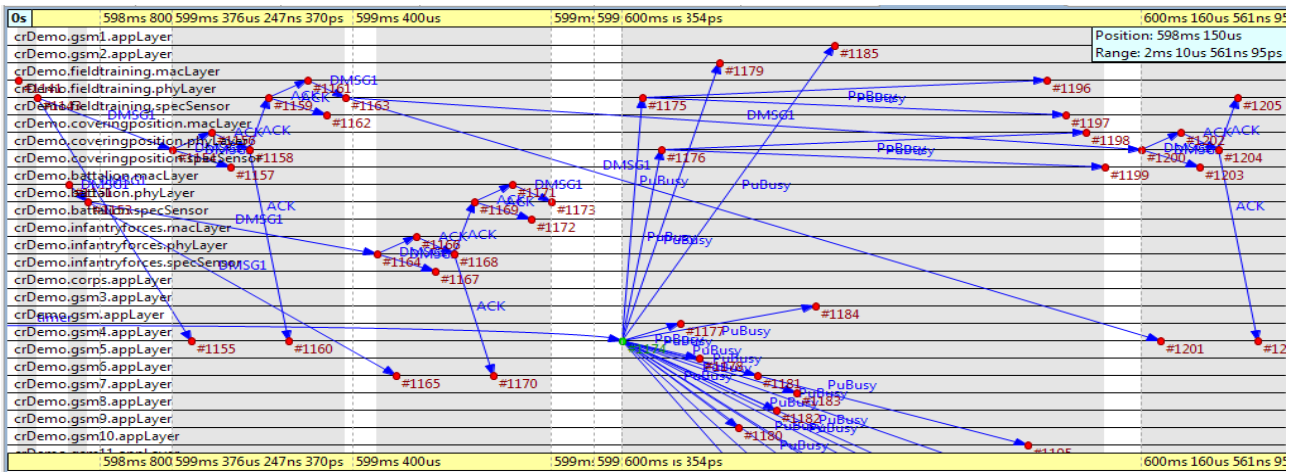


Figure 4.17 : Behaviors of CRNs Elements of the RSA Case Study in Log File .

While the Noise-Jamming attack of the RSA case study of the main simulation parameters showed in Table 4.15, and The Figure 4.18.

Table 4.15: Noise-jamming Attack within the RSA Case Study.

Throughput in Mbps	Data Drop Rate in Mbps	Detection Time in Seconds	Delay Time in Seconds
0.615	0.352	1.453	0.402

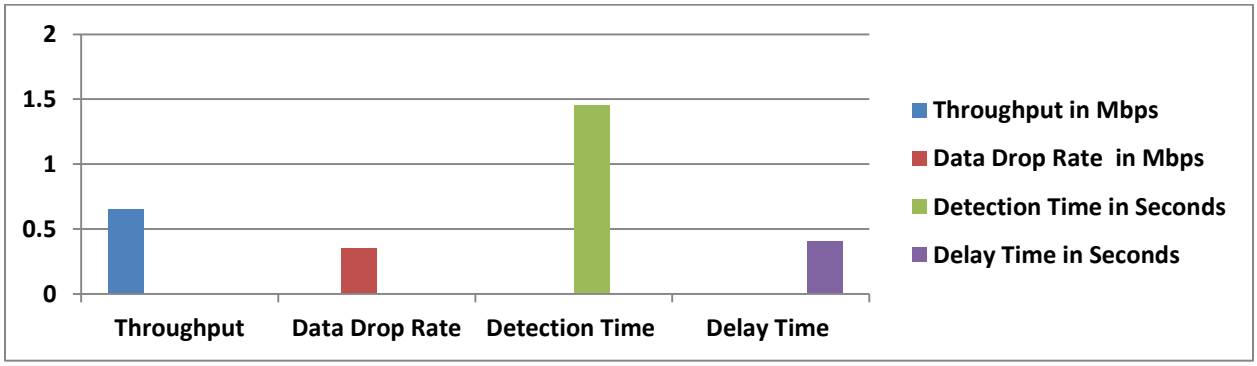


Figure 4.18: Throughput, Data Drop Rate, Detection Time and Delay Time of Noise-Jamming Attack within RSA Case Study.

4.2.3 Case Study of FHSS and RSA in Cognitive Radio Network

In this case study, we simulate CRNs with Frequency hopping spread spectrum (FHSS) and The Rivest-Shamir-Adleman (RSA) algorithm as a compound system to enhance the security of cognitive radio network system. The simulation parameters used as the same cases for previous case studies. The Table 4.16, summarized signals for application layer , MAC layer and spectrum sensing that's collect interconnection layers (phy-mac layer) in all transmitter nodes as (battalion, corps and fieldtraining).

Table 4.16: Application Layer Request, Mac Layer and Spectrum Sensing Values from all Transmitter Nodes within RSA-FHSS Case Study.

Application Layer		**MAC Layer**		**Spectrum Sensing**	
appRequest	**0-22**	rtsFailSignal	**0-1**	sensingSignal	**10-32**
		rtsSignal	**6-28**		
		handover	**0-4**		

Besides, the Figure 4.19, shows the Application Layer Request, Mac Layer and Spectrum Sensing values from all transmitter nodes as (battalion, corps and fieldtraining)

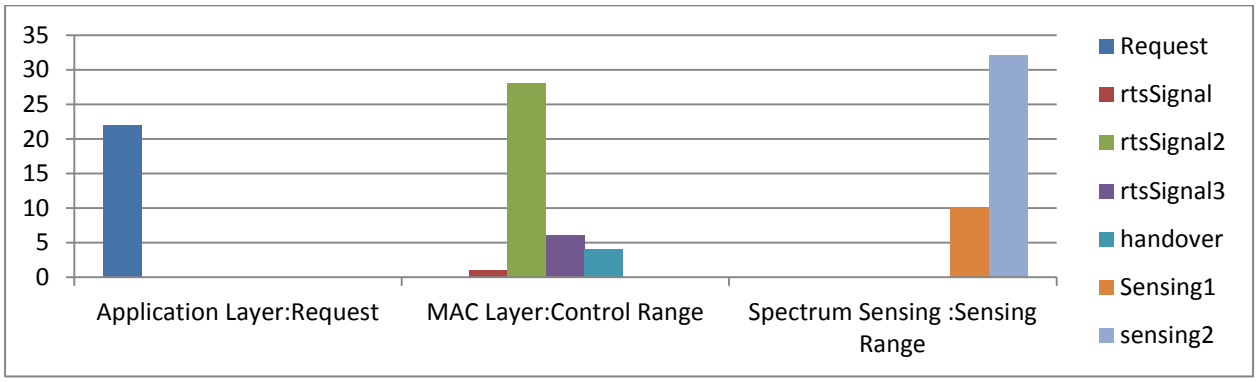


Figure 4.19: Application Layer Request, Mac Layer and Spectrum Sensing Values from all Transmitter Nodes within RSA-FHSS Case Study.

The Table 4.17, summarizes the results for the data and sensing signals in all Receiver nodes as (infantryforces, combatteam and coveringposition).

Table 4.15 : MAC Layer NACKs and Spectrum Sensing from all Receiver Nodes within RSA-FHSS Case Study.

MAC Layer NACKs		**Spectrum Sensing**	
NACKsSignal	**0-3**	sensingSignal	**21-57**

While, Figure 4.20, shows results statics for all receiver nodes.

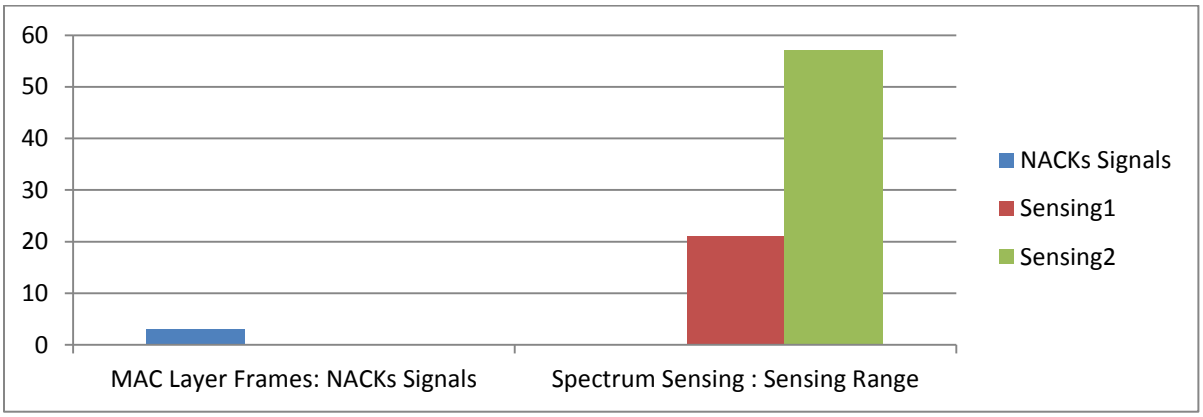


Figure 4.20: MAC Layer NACKs and Spectrum Sensing from all Receivers Nodes within RSA-FHSS Case Study .

The Table 4.18, showed the number of transmission and reception data frames messages from all transmitters and receivers nodes.

Table 4.18 : Sent and Received Data Messages for the RSA-FHSS Case Study.

CR Transmitter nodes	**Sent Data messages**	**Sum**	CR Receiver nodes	**Received Data messages**	**Sum**
corps	447	1019	combatteam	391	903
battalion	293		infantryforces	239	
fieldtraining	279		coveringposition	273	

While Table 4.19, and Figure 4.21, explained the main simulation parameters used for comparison with all case studies and this table for the RSA-FHSS case study implementation based on the simulation parameters values created in Table 4.16 above.

Table 4.19 : The main Simulation Parameters for the RSA-FHSS Case Study.

Throughput in Mbps	Data Drop Rate in Mbps	Detection Time in Seconds	Delay Time in Seconds
0.886	0.113	0.567	0.282

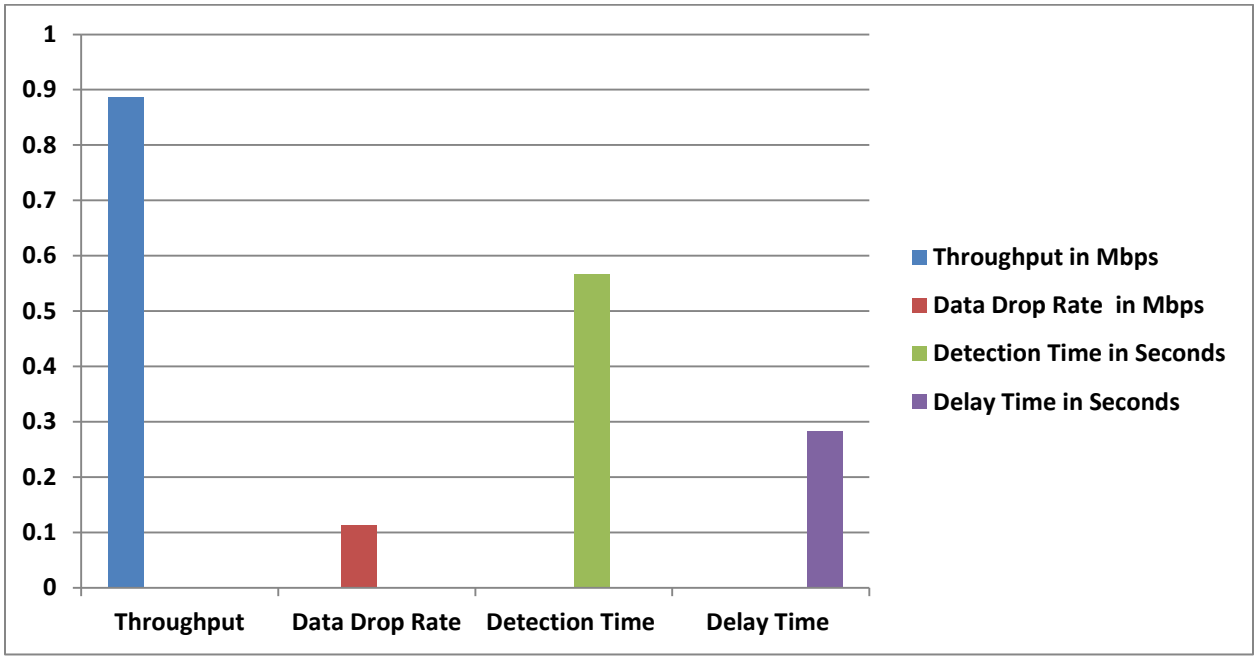


Figure 4.21 : Throughput, Data drop rate, detection time and Delay Time for RSA-FHSS Case Study.

Each of these results based on signals from MAC Layer because this layer have the implementation of frame data signal that represents data rate spectrum exchange among cognitive radio nodes for all case studies.

We note from Log file in this case study using some nodes to the channel and take the time of another node through exploit carrier medium(channel). The Figure 4.22, some of parameters selected to show for this case study from log file,

Through, entire simulation time for all cognitive radio elements represented by (20 primary users, 6 secondary users).

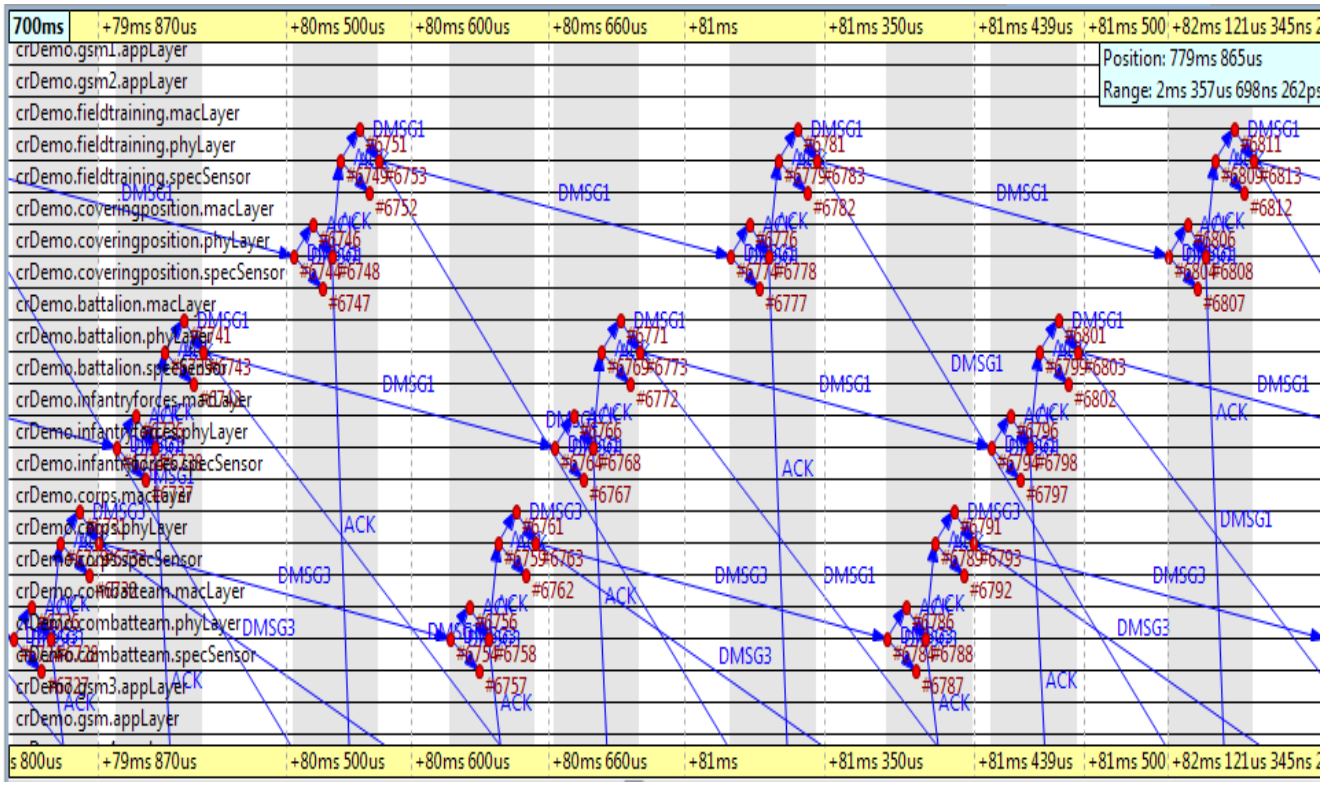


Figure 4.22: The Log File of the RSA-FHSS Case Study .

While the Noise-Jamming attack results for all simulation parameters of the RSA-FHSS case study build as follow :

Table 4.20 : Noise attack with RSA-FHSS Case Study.

Throughput in Mbps	Data Drop Rate in Mbps	Detection Time in Seconds	Delay Time in Seconds
0.841	0.118	0.595	0.296

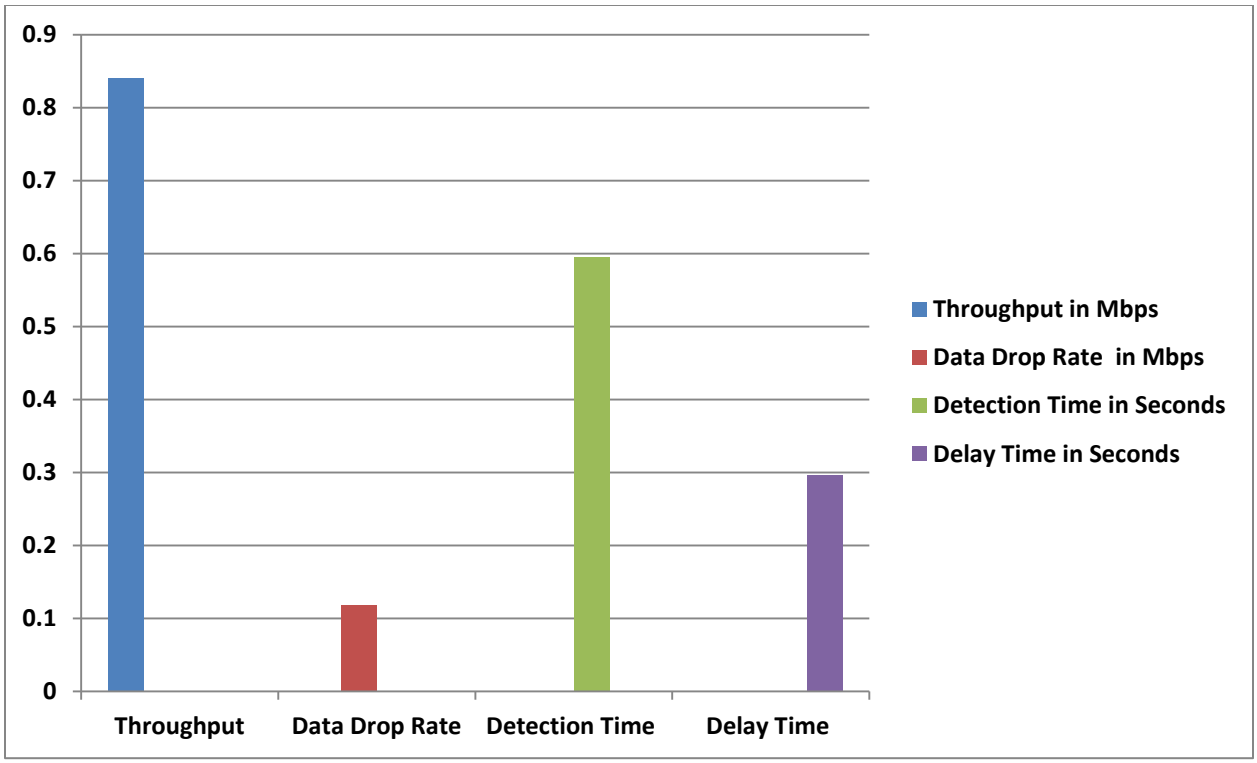


Figure 4.23 : Throughput, Data drop rate, detection time and Delay Time of Noise attack within RSA-FHSS Case Study.

The proposed system is explained and it compared with other states based on the same simulation parameters as Throughput, Data drop, detection time and delay time. The Figure 4.24, shows parameters comparisons for all proposed cases studies based on the data message generated from all transmitters / receivers nodes in each case study.

While the Figure 4.25, shows the same simulation parameters with all case studies within the state of Noise-Jamming Attack and how it effects on the Throughput by reducing the transmission date rate and increase the data drop rate, detection time and delay time which it effects overall the network performance.

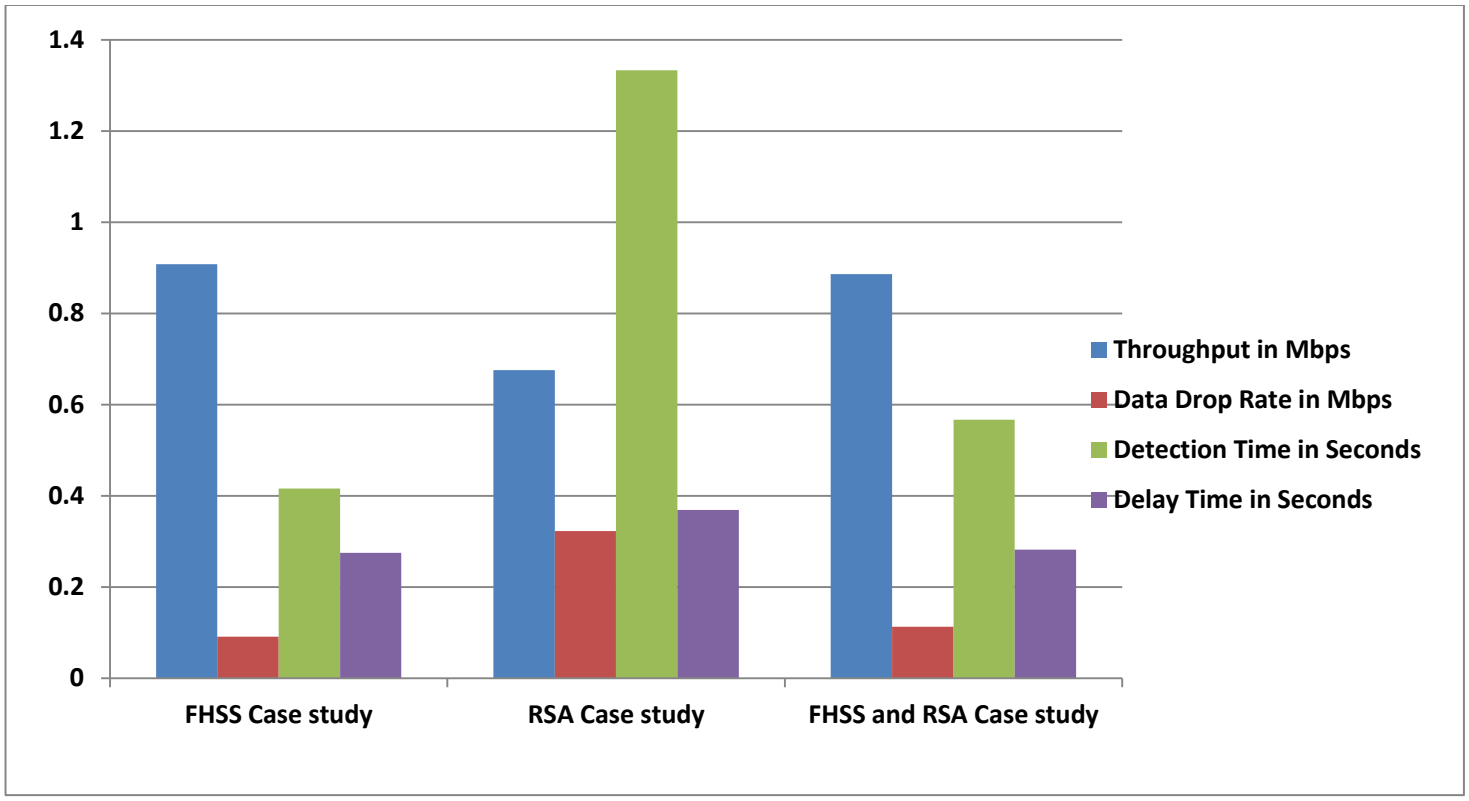


Figure 4.24: Comparisons of the used Three Cases Studies .

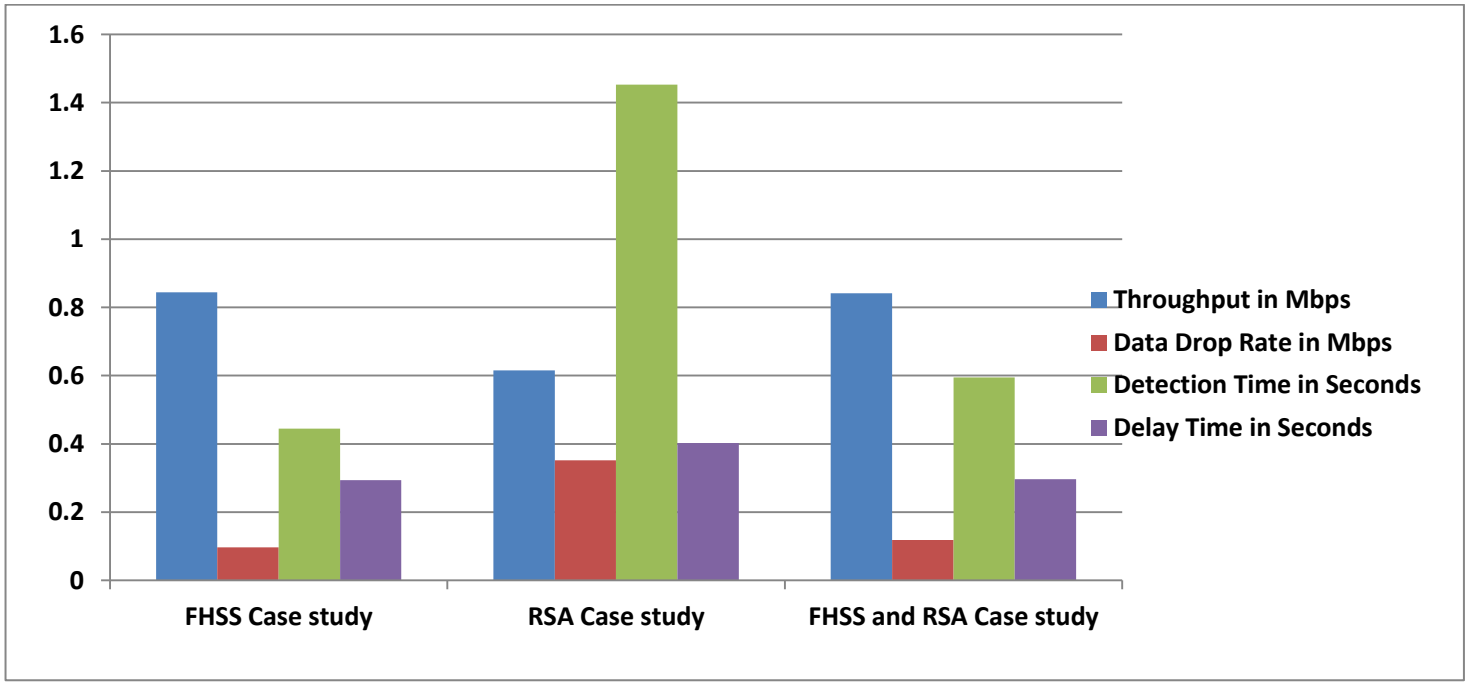


Figure 4.25: Comparisons of the used Three Cases Studies with Noise-Jamming Attack .

The Table 4.21, and Table 4.22, showed the simulation parameters of case studies without Noise-Jamming attack and with Noise-Jamming attack states.

Table 4.21: Without Noise-Jamming Attack State.

Without Noise-Jamming				
Simulation Parameters Case Studies	**Throughput in Mbps**	**Data Drop Rate in Mbps**	**Detection Time in Seconds**	**Delay Time in Seconds**
FHSS Case study	0.908	0.091	0.416	0.275
RSA Case study	0.676	0.323	1.333	0.369
FHSS and RSA Case study	0.886	0.113	0.567	0.282

Table 4.21: With Noise-Jamming Attack State.

With Noise-Jamming Attack				
Simulation Parameters Case Studies	**Throughput in Mbps**	**Data Drop Rate in Mbps**	**Detection Time in Seconds**	**Delay Time in Seconds**
FHSS Case study	0.844	0.097	0.445	0.294
RSA Case study	0.615	0.352	1.453	0.402
FHSS and RSA Case study	0.841	0.118	0.595	0.296

CHAPTER FIVE

Conclusions and Future works

5.1 Conclusions

1. The proposed system simulates the security system with (6 CR or Secondary Users) labeled as military units and (20 Primary Users) placed as a licensed frequency band GSM units.
2. Simulating CRNs in Military Application considered as challenges because this considers the critical direction and has more secrecy from researchers and specialization peoples.
3. Developing a Cryptosystem to enhance the security of CRNs by implementing:
   - Public-key encryption methods called Rivest, Shamir, and Adelman (RSA)
   - Adapting method based on Spread-spectrum techniques like a Frequency hopping spread spectrum (FHSS).
4. The proposed system enhancing Cognitive Radio (CR) based on the simulation parameters: Throughput, Data Drop Rate, Detection Time and Delay Time simulation parameters.
5. The used system gives more throughput rate result in case FHSS within CRNs as the maximum throughput in Mbps (0.908) while in RSA implementation as (0.676 Mbps) and within compound system as (0.886 Mbps).
6. The used system based on the spread spectrum technique (FHSS) has a range of frequencies as twenty frequencies bands described as the (idle channel) for transmission suggested by the Spectrum Sensor module of the used system within OMNET++. The used idle channel changed randomly based on the spectrum pool suggested (20 bands) and check specific threshold value programmed as interference state so when the value arrived at the same threshold value the counter hop to the next frequency band. So it

is difficult to interference or jamming to a specific spectrum band within the proposed idle channel.

7. Implementing three Messages types in OMNET++ as (Acknowledgment, Control for control channel purpose and Data messages for transmission data units) and the encryption text (cipher-text) equivalent text in C# of Data message frame format encrypted with RSA security algorithm.
8. The collision was mitigated due to implement Request To Send/Clear To Send protocol setting in MAC Layer through this method used to make channel provided clear to transmission data and it doesn't collision to happened based on acknowledgment state .
9. Data Drop Rate was the maximum rate in the second case study due to verification and checking period and decreased a number of available channels for transmission and the value is (0.323) and the second value with the compound system based on the RSA and FHSS as the third state is (0.113), while the first case study as FHSS in CRNs recorded (0.091) as the better state.
10. Simulating Noise-Jamming attack in CRNs environment in all case studies where the used system presents the Noise-Jamming attack effects by decreased Throughput , increased data drop rate, detection Time and delay Time, so It can easily disrupt a network.

5.2 Suggestions for Future Works

1. Employing a Game Theory approach to networking, commonly to resolve routing and resource allocation problems, power management, and security issues in an ambitious critical environment.

2. Applying the proposed system on other types of data type such as video, voice and files.
3. Using another type of Cryptography scheme and relating concept reviewed in literatures survey like (AES, ECC, RC5, A5).
4. Implementing the encryption algorithm inside the same security system libraries as the data encryption executed within simulation environment and reduce the use of outside frameworks such as crypto libraries from another simulation or programing tools.

REFERENCES

[1] Butt, M. A. (2013). Cognitive radio network: Security enhancements. *Journal of Global Research in Computer Science*, *4*(2), 36-41.

[2] Kokare, S., & Kamble, R. D. (2014). Spectrum Sensing Techniques in Cognitive Radio Cycle. *International Journal of Engineering Trends and Technology (IJETT)*, *9*(1), 16-20.

[3] Baldini, G., Sturman, T., Biswas, A. R., Leschhorn, R., Godor, G., & Street, M. (2011). Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. *IEEE Communications Surveys & Tutorials*, *14*(2), 355-379.

[4] Shuaib, K., Barka, E., Al Hussien, N., Abdel-Hafez, M., & Alahmad, M. (2016). Cognitive radio for smart grid with security considerations. *Computers*, *5*(2), 7.

[5] Polson, J. (2004, November). Cognitive radio applications in software defined radio. In *Proceedings of the SDR Forum Conference 2004*.

[6] Singh, S., Mushtaq, G., Tiwari, N. K., & Singh, A. P. (2015). Cognitive Radio With Software Defined Radio and Mimo for Future Generation Wireless Communication. *Journal of Computer Science System Biology*.

[7] Mahmoud, Q. (Ed.). (2007). *Cognitive networks: towards self-aware networks*. John Wiley & Sons.

[8] Hu, W., Willkomm, D., Abusubaih, M., Gross, J., Vlantis, G., Gerla, M., & Wolisz, A. (2007). Cognitive radios for dynamic spectrum access-dynamic frequency hopping communities for efficient IEEE 802.22 operation. *IEEE Communications Magazine*, *45*(5), 80-87.

[9] Li, X., & Hwu, J. (2009, April). A frequency hopping spread spectrum transmission scheme for uncoordinated cognitive radios. In *2009 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 2345-2348). IEEE.

[10] Cheng, Z., Wang, S., Qu, X., Yan, S., Hu, F., & Li, A. (2009, October). CogDFH-a Cognitive-Based differential frequency hopping network. In *MILCOM 2009-2009 IEEE Military Communications Conference* (pp. 1-7). IEEE.

[11] Muraleedharan, R. (2011). Cognitive security framework for heterogeneous sensor network using swarm intelligence.

[12] Harbin, J. R. (2011). *Security Strategies In Wireless Sensor Networks* (Doctoral dissertation, University of York).

[13] León Abarca, O. (2012). Contributions to the security of cognitive radio networks.

[14] Parvin, S., Hussain, F. K., & Hussain, O. K. (2013). Conjoint trust assessment for secure communication in cognitive radio networks. *Mathematical and Computer Modelling*, *58*(5-6), 1340-1350.

[15] Khasawneh, M., & Agarwal, A. (2014, March). A survey on security in Cognitive Radio networks. In *2014 6th International Conference on Computer Science and Information Technology (CSIT)* (pp. 64-70). IEEE.

[16] Jain, A., Sharma, V., & Amrutur, B. (2014, February). Soft real time implementation of a Cognitive Radio testbed for frequency hopping primary satisfying QoS requirements. In *2014 Twentieth National Conference on Communications (NCC)* (pp. 1-6). IEEE.

[17] Yan, Q. (2014). *Security Enhanced Communications in Cognitive Networks* (Doctoral dissertation, Virginia Tech).

[18] Tang, H., & Watson, S. (2014). *Cognitive radio networks for tactical wireless communications*. Defence Research and Development Canada-Ottawa Research Centre Ottawa, Ontario Canada.

[19] Nanthini, S. B., Hemalatha, M., Manivannan, D., & Devasena, L. (2014). Attacks in cognitive radio networks (CRN)-A survey. *Indian Journal of Science and Technology*, *7*(4), 530.

[20] Sundararajan, M., & Govindaswamy, U. (2014). Multicarrier spread spectrum modulation schemes and efficient FFT algorithms for cognitive radio systems. *Electronics*, *3*(3), 419-443.

[21] Kärkkäinen, A. (2015). Developing cyber security architecture for military networks using cognitive networking.

[22] Dabcevic, K. (2015). Intelligent jamming and anti-jamming techniques using Cognitive Radios. *PhD Programme in Computational Intelligence University of Genoa*.

[23] Kaur, N., Aulakh, I. K., & Vig, R. (2016). Analysis of spread spectrum techniques in cognitive radio networks. *International Journal of Applied Engineering Research*, *11*(8), 5641-5645.

[24] Zou, C., & Chigan, C. (2016). Dynamic spectrum access-based cryptosystem for cognitive radio networks. *Security and Communication Networks*, *9*(17), 4151-4165.

[25] Li, Y., Han, C., Wang, M., Chen, H., & Xie, L. (2016, October). A primary user emulation attack detection scheme in cognitive radio network with mobile secondary user. In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)* (pp. 1076-1081). IEEE.

[26] Wu, H., Sun, X., Guo, C., & Ren, S. (2016, December). Malicious user detection for wide-band cognitive radio networks. In *2016 Asia-Pacific Microwave Conference (APMC)* (pp. 1-4). IEEE.

[27] Hamood, A. S., & Sadkhan, S. B. (2017, December). Keywords Sensitivity Recognition of Military Applications in Secure CRNs Environments. In *2017 Second Al-Sadiq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)* (pp. 96-101). IEEE.

[28] Salahdine, F. (2017). Spectrum sensing techniques for cognitive radio networks. *arXiv preprint arXiv:1710.02668*.

[29] Elanagai, G., & Jayasri, C. Network Security Based Data Televising by Fraternization Spectrum Sensing in Cognitive Radio Network.

[30] Zarif, N. S., Moghadam, A. Q., & Imani, M. (2018). Hybrid Technique for Spectrum Sharing in Cognitive Radio Networks for the Internet of Things. *International Journal of Computer Applications*, *975*, 8887.

[31] B.Sarala, S.Rukmani Devi, M.Suganthy, S.Jhansi Ida, "A Novel Authentication Mechanism for Cognitive Radio Network", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019.

[32] Xiang, Z., Yang, W., Pan, G., Cai, Y., & Song, Y. (2019). Physical layer security in cognitive radio inspired NOMA network. *IEEE Journal of Selected Topics in Signal Processing*, *13*(3), 700-714.

[33] Mitola, J. (1999, November). Cognitive radio for flexible mobile multimedia communications. In *1999 IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99)(Cat. No. 99EX384)* (pp. 3-10). IEEE.

[34] Pandit, S., & Singh, G. (2017). Cognitive radio communication system: spectrum sharing techniques. In *Spectrum Sharing in Cognitive Radio Networks* (pp. 1-33). Springer, Cham.

[35] Chen, K. C., & Prasad, R. (2009). Cognitive Radio Communications.

[36] Perera, L. N. T., & Herath, H. M. V. R. (2011, August). Review of spectrum sensing in cognitive radio. In *2011 6th international conference on industrial and information systems* (pp. 7-12). IEEE.

[37] Masonta, M. T., Mzyece, M., & Ntlatlapa, N. (2012). Spectrum decision in cognitive radio networks: A survey. *IEEE Communications Surveys & Tutorials*, *15*(3), 1088-1107.

[38] Doerr, C., Grunwald, D., & Sicker, D. C. (2009). Local control of cognitive radio networks. *annals of telecommunications-annales des télécommunications*, *64*(7-8), 503-534.

[39] Cabric, D., Mishra, S. M., & Brodersen, R. W. (2004, November). Implementation issues in spectrum sensing for cognitive radios. In *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.* (Vol. 1, pp. 772-776). Ieee.

[40] Hwang, J., Saki, H., & Shikh-Bahaei, M. (2017, September). Adaptive modulation and coding and cooperative arq in a cognitive radio system. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 310-315). IEEE.

[41] Qiao, D., & Choi, S. (2006). New 802.11 h mechanisms can reduce power consumption. *IT Professional*, *8*(2), 43-48.

[42] Shah, M. A., Zhang, S., Kamran, M., Javaid, Q., & Fatima, B. (2016). A survey on MAC protocols for complex self-organizing cognitive radio networks. *Complex Adaptive Systems Modeling*, *4*(1), 18.

[43] López-Benítez, M. (2018). Overview of Recent Applications of Cognitive Radio in Wireless Communication Systems. *Handbook of Cognitive Radio. Springer, Singapore*.

[44] Cognitive Radio Work Group , "Quantifying the Benefits of Cognitive Radio",WINNF-09-P-0012-V1.0.0, 2010.

[45] Jayapalan, A., & Karuppasamy, T. (2018). Spectrum Sensing and Mitigation of Primary User Emulation Attack in Cognitive Radio. In *Cognitive Radio in 4G/5G Wireless Communication Systems*. IntechOpen.

[46] Amjad, M., Musavian, L., & Rehmani, M. H. (2019). Effective capacity in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *21*(4), 3007-3038.

[47] Mohapatra, H., & VSSUT, B. Survey on challenges in Cognitive Radio, 2018.

[48] Ali, A., Iqbal, M., Baig, A., & Wang, X. (2011). Routing techniques in cognitive radio networks: A survey. *International Journal of Wireless & Mobile Networks*, *3*(3), 96-110.

[49] Numan, P. E., Yusof, K. M., Suleiman, D. U., Bassi, J. S., Yusof, S. K. S., & Din, J. B. (2016). Hidden node scenario: A case for cooperative spectrum sensing in cognitive radio networks. *Indian Journal of Science and Technology*, *9*(46).

[50] Wang, F., Krunz, M., & Cui, S. (2008, April). Spectrum sharing in cognitive radio networks. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications* (pp. 1885-1893). IEEE.

[51] Clancy, C., Hecker, J., Stuntebeck, E., & O'Shea, T. (2007). Applications of machine learning to cognitive radio networks. *IEEE Wireless Communications*, *14*(4), 47-52.

[52] Mathur, C. N., & Subbalakshmi, K. P. (2007). Security issues in cognitive radio networks. *Cognitive Networks*, *25*, 272-290.

[53] Ahmed, M., Hailes, S., Kolar, V., Petrova, M., & Mahonen, P. (2009, June). A component-based architecture for cognitive radio resource management. In *2009 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications* (pp. 1-6). IEEE.

[54] Kumar, T. P., Suresh, E., Ramana, B. V., & Shashank, B. S. Survey: Routing Protocols in Cognitive Radio Mesh Networks. *vol*, *6*, 603-608.

[55] Mansoor, N., Islam, A. M., Zareei, M., Baharun, S., Wakabayashi, T., & Komaki, S. (2015). Cognitive radio ad-hoc network architectures: a survey. *Wireless Personal Communications*, *81*(3), 1117-1142.

[56] Chen, K. C., Peng, Y. J., Prasad, N., Liang, Y. C., & Sun, S. (2008, January). Cognitive radio network architecture: part I--general structure. In *Proceedings of the 2nd international conference on Ubiquitous information management and communication* (pp. 114-119).

[57] Shah, M. A., Zhang, S., Kamran, M., Javaid, Q., & Fatima, B. (2016). A survey on MAC protocols for complex self-organizing cognitive radio networks. *Complex Adaptive Systems Modeling*, *4*(1), 18.

[58] Joshi, G. P., Nam, S. Y., & Kim, S. W. (2013). Cognitive radio wireless sensor networks: applications, challenges and research trends. *Sensors*, *13*(9), 11196-11228.

[59] Zhang, Q., Kokkeler, A. B., & Smit, G. J. (2006). Cognitive Radio for Emergency Networks. *Mobile Multimedia: Communication Engineering Perspective*.

[60] Zeng, F., & Xu, J. (2016). Leasing-based performance analysis in energy harvesting cognitive radio networks. *Sensors*, *16*(3), 305.

[61] Ghafoor, S., Sutton, P. D., Sreenan, C. J., & Brown, K. N. (2014). Cognitive radio for disaster response networks: survey, potential, and challenges. *IEEE Wireless Communications*, *21*(5), 70-80.

[62] Li, B., Fei, Z., & Zhang, Y. (2018). UAV communications for 5G and beyond: Recent advances and future trends. *IEEE Internet of Things Journal*, *6*(2), 2241-2263.

[63] Joshi, G. P., Nam, S. Y., & Kim, S. W. (2013). Cognitive radio wireless sensor networks: applications, challenges and research trends. *Sensors*, *13*(9), 11196-11228.

[64] Nadeem, S., Rizwan, M., Ahmad, F., & Manzoor, J. (2019). Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, *10*(1), 288-295.

[65] Baldini, G., Sturman, T., Biswas, A. R., Leschhorn, R., Godor, G., & Street, M. (2011). Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. *IEEE Communications Surveys & Tutorials*, *14*(2), 355-379.

[66] Hlavacek, D., & Chang, J. M. (2014). A layered approach to cognitive radio network security: A survey. *Computer Networks*, *75*, 414-436.

[67] Axelsson, S. (2000). *Intrusion detection systems: A survey and taxonomy* (Vol. 99). Technical report.

[68] Dubey, R., Sharma, S., & Chouhan, L. (2013). Security for cognitive radio networks. In *Cognitive Radio and Interference Management: Technology and Strategy* (pp. 238-256). IGI Global.

[69] Kärkkäinen, A. (2015). Developing cyber security architecture for military networks using cognitive networking.

[70] Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. *Frontiers in psychology*, *9*, 691.

[71] Zhang, X., & Li, C. (2010). Constructing secured cognitive wireless networks: experiences and challenges. *Wireless Communications and Mobile Computing*, *10*(1), 50-69.

[72] Mishra, A., Nadkarni, K., & Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. *IEEE wireless communications*, *11*(1), 48-60.

[73] Khasawneh, M., & Agarwal, A. (2014, March). A survey on security in Cognitive Radio networks. In *2014 6th International Conference on Computer Science and Information Technology (CSIT)* (pp. 64-70). IEEE.

[74] Buccardo, A. (2010). A signal detector for cognitive radio system.

[75] Shu, Z., Qian, Y., & Ci, S. (2013). On physical layer security for cognitive radio networks. *IEEE Network*, *27*(3), 28-33.

[76] El-Hajj, W., Safa, H., & Guizani, M. (2011). Survey of security issues in cognitive radio networks. *Journal of Internet Technology*, *12*(2), 181-198.

[77] Hlavacek, D., & Chang, J. M. (2014). A layered approach to cognitive radio network security: A survey. *Computer Networks*, *75*, 414-436.

[78] Hernandez-Serrano, J., León, O., & Soriano, M. (2011). Modeling the lion attack in cognitive radio networks. *EURASIP Journal on Wireless Communications and Networking*, *2011*, 1-10.

[79] Yu, Y. C., Hu, L., Li, H. T., Zhang, Y. M., Wu, F. M., & Chu, J. F. (2014). The security of physical layer in cognitive radio networks. *J Commun*, *9*(12), 28-33.

[80] Goldsmith, A., Jafar, S. A., Maric, I., & Srinivasa, S. (2009). Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. *Proceedings of the IEEE*, *97*(5), 894-914.

[81] Clancy, T. C., & Goergen, N. (2008, May). Security in cognitive radio networks: Threats and mitigation. In *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)* (pp. 1-8). IEEE.

[82] Zhang, L., Ding, G., Wu, Q., Zou, Y., Han, Z., & Wang, J. (2015). Byzantine attack and defense in cognitive radio networks: A survey. *IEEE Communications Surveys & Tutorials*, *17*(3), 1342-1363.

[83] Bian, K., & Park, J. M. (2006, August). MAC-layer misbehaviors in multi-hop cognitive radio networks. In *2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006)* (pp. 228-248).

[84] Zhu, L., & Zhou, H. (2008, December). Two types of attacks against cognitive radio network MAC protocols. In *2008 International Conference on Computer Science and Software Engineering* (Vol. 4, pp. 1110-1113). IEEE.

[85] Raut, R., Sawant, R., & Madbushi, S. (2020). *Cognitive Radio: Basic Concepts, Mathematical Modeling and Applications*. CRC Press.

[86] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad hoc networks*, *1*(2-3), 293-315.

[87] Dudley, S. M., Headley, W. C., Lichtman, M., Imana, E. Y., Ma, X., Abdelbar, M., ... & Reed, J. H. (2014). Practical issues for spectrum management with cognitive radios. *Proceedings of the IEEE*, *102*(3), 242-264.

[88] Butt, M. A. (2013). Cognitive radio network: Security enhancements. *Journal of Global Research in Computer Science*, *4*(2), 36-41.

[89] Zhao, J., & Cao, G. (2014). Robust topology control in multi-hop cognitive radio networks. *IEEE Transactions on mobile computing*, *13*(11), 2634-2647.

[90] Wang, W., Sun, Y., Li, H., & Han, Z. (2010, December). Cross-layer attack and defense in cognitive radio networks. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010* (pp. 1-6). IEEE.

[91] Sen, J. (2013). A survey on security and privacy protocols for cognitive wireless sensor networks. *arXiv preprint arXiv:1308.0682*.

[92] Zubair, S., Fisal, N., Baguda, Y. S., & Saleem, K. (2013). Assessing routing strategies for cognitive radio sensor networks. *Sensors*, *13*(10), 13005-13038.

[93] Wang, Y., Yu, F. R., Tang, H., & Huang, M. (2014). A mean field game theoretic approach for security enhancements in mobile ad hoc networks. *IEEE transactions on wireless communications*, *13*(3), 1616-1627.

[94] Chakraborty, T., Misra, I. S., & Prasad, R. (2019). *VoIP Technology: Applications and Challenges*. Springer International Publishing.

[95] Tang, K., Tang, W., Luo, E., Tan, Z., Meng, W., & Qi, L. (2020). Secure Information Transmissions in Wireless-Powered Cognitive Radio Networks for Internet of Medical Things. *Security and Communication Networks*, *2020*.

[96] Kurt, G. K., & Cepheli, Ö. (2020). Physical Layer Security of Cognitive IoT Networks. In *Towards Cognitive IoT Networks* (pp. 101-123). Springer, Cham.

[97] Tarek, D., Benslimane, A., Darwish, M., & Kotb, A. M. (2020). Survey on spectrum sharing/allocation for cognitive radio networks Internet of Things. *Egyptian Informatics Journal*.

[98] Swayamsiddha, S., & Mohanty, C. (2020). Application of cognitive Internet of Medical Things for COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*.

[99] Arshid, K., Hussain, I., Bashir, M. K., Naseem, S., Ditta, A., Mian, N. A., ... & Khan, I. A. (2020). Primary User Traffic Pattern Based Opportunistic Spectrum Handoff in Cognitive Radio Networks. *Applied Sciences*, *10*(5), 1674.

[100] Khan, M. S., Gul, N., Kim, J., Qureshi, I. M., & Kim, S. M. (2020). A Genetic Algorithm-Based Soft Decision Fusion Scheme in Cognitive IoT Networks with Malicious Users. *Wireless Communications and Mobile Computing*, *2020*.

[101] Tripathi, A. K., Potnis, A. A., & Pushpad, A. (2016). A Review On Frequency Hopping Spread Spectrum Based Anti-Jamming Improvement with Encrypted Spreading Codes.

[102] Kak, A. (2017). Lecture Notes on "Computer and Network Security: Lecture 8: AES: The Advanced Encryption Standard". *Purdue University*.

[103] Milanov, E. The RSA Algorithm, 2009.

[104] Kak, A. (2017). Lecture Notes on "Computer and Network Security: Lecture 12: Public-Key Cryptography and the RSA Algorithm". *Purdue University*.

[105] Aryanti, A., & Mekongga, I. (2018). Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher In Web Based Information System. In *E3S Web of Conferences* (Vol. 31, p. 10007). EDP Sciences.

[106] Cadeau, W., & Li, X. (2012, March). Anti-jamming performance of cognitive radio networks under multiple uncoordinated jammers in fading environment. In *2012 46th Annual Conference on Information Sciences and Systems (CISS)* (pp. 1-6). IEEE.

[107] Rathee, G., Ahmad, F., Kerrache, C. A., & Azad, M. A. (2019). A Trust Framework to Detect Malicious Nodes in Cognitive Radio Networks. *Electronics*, *8*(11), 1299.

[108] Al-Ali, A., & Chowdhury, K. (2014, June). Simulating dynamic spectrum access using ns-3 for wireless networks in smart environments. In *2014 eleventh annual IEEE international conference on sensing, communication, and networking workshops (SECON workshops)* (pp. 28-33). IEEE.

[109] Palacios, P., & Castro, A. (2018). Cognitive Radio Simulator for Mobile Networks: Design and Implementation. *i-Manager's Journal on Communication Engineering and Systems*, *7*(2), 1.

[110] Yawada, P. S., & Dong, M. T. (2019). Intelligent process of spectrum handoff/mobility in cognitive radio networks. *Journal of Electrical and Computer Engineering*, *2019*.

[111] Xiao, Y., & Hu, F. (Eds.). (2008). *Cognitive radio networks*. CRC press.

[112] Soliman, J. N., Mageed, T. A., & El-Hennawy, H. M. (2017, December). Digital signature and authentication mechanisms using new customized hash function for cognitive radio networks. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)* (pp. 175-181). IEEE.

[113] Ohaeri, I., Ekabua, O., Isong, B., Esiefarienrhe, M., & Motojane, M. (2015). Mitigating Intrusion and Vulnerabilities in Cognitive Radio Networks. *Advances in Computer Science: an International Journal*, *4*(3), 1-10.

[114] Rodriguez, P. M., Lizeaga, A., Mendicute, M., & Val, I. (2019). Spectrum handoff strategy for cognitive radio-based MAC for real-time industrial wireless sensor and actuator networks. *Computer Networks*, *152*, 186-198.

[115] Sen, J. (2013). A survey on security and privacy protocols for cognitive wireless sensor networks. *arXiv preprint arXiv:1308.0682*.

[116] Sun, H., & Han, H. (2019). Analysis of Spectrum Selection Methods based on Platform-Qualnet in Cognitive Radio Networks. *International Journal of Online and Biomedical Engineering (iJOE)*, *15*(03), 124-133.

[117] Di Renzo, M., Graziosi, F., & Santucci, F. (2009, April). Cooperative spectrum sensing in cognitive radio networks over correlated log-normal shadowing. In *VTC Spring 2009-IEEE 69th Vehicular Technology Conference* (pp. 1-5). IEEE.

[118] Shukla, P. A., & Gour, P. (2017). An optimized sensing and Detection of Cognitive Radio Network using Monte Carlo Simulation. *International Journal of Computer Applications*, *162*(4).

[119] Zhang, J., Cai, L., & Zhang, S. (2017). Malicious cognitive user identification algorithm in centralized spectrum sensing system. *Future Internet*, *9*(4), 79.

[120] Singhal, P., Sharma, P., & Rizvi, S. (2019). Thwarting Sybil Attack by CAM Method in WSN using Cooja Simulator Framework. *International Journal of Engineering & Technology*, *8*(1.5), 116-125.

[121] Kurose, J. F. (2005). *Computer networking: A top-down approach featuring the internet, 3/E*. Pearson Education India.

[122] Chen, K. C., Peng, Y. J., Prasad, N., Liang, Y. C., & Sun, S. (2008, January). Cognitive radio network architecture: part I--general structure. In *Proceedings of the 2nd international conference on Ubiquitous information management and communication* (pp. 114-119).

[123] Ajay Kumar Gautam, "cognitive Radio Networks",(Roll No. P08EC901), 2009.

[124] Chang, K. W., & Lee, W. J. (2011). *U.S. Patent No. 7,933,358*. Washington, DC: U.S. Patent and Trademark Office.

[125] Dong, Q., Chen, Y., Li, X., & Zeng, K. (2018). A Survey on Simulation Tools and Testbeds for Cognitive Radio Networks Study. *arXiv preprint arXiv:1808.09858*.

[126] Khan, S. N., Kalil, M. A., & Mitschele-Thiel, A. (2013, April). crSimulator: A discrete simulation model for cognitive radio ad hoc networks in OMNeT++. In *6th Joint IFIP Wireless and Mobile Networking Conference (WMNC)* (pp. 1-7). IEEE.

[127] Labiod, H., Afifi, H., & De Santis, C. (2007). *Wi-FiTM, BluetoothTM, ZigBeeTM and WiMaxTM*. Springer Science & Business Media.

[128] Ullah, S., Hassan, M. M., Hossain, M. S., & Alelaiwi, A. (2020). Performance Evaluation of RTS/CTS Scheme in Beacon-Enabled IEEE 802.15. 6 MAC Protocol for Wireless Body Area Networks. *Sensors*, *20*(8), 2368.

[129] Merlin, S., Abraham, S. P., Frederiks, G. R., Jones, V. K., & Wentink, M. M. (2015). *U.S. Patent No. 9,119,110*. Washington, DC: U.S. Patent and Trademark Office.

الخلاصة

الراديو الادراكي (CR) هو تكنولوجيا استخدام نطاق الطيف الحر المستخدم بناءً على العناصر الرئيسية كالمستخدمين الاساسي والثانوي ، وذلك من خلال قدرة الهيكل أن يتحسس للبيئة المحيطة به ويتكيف مع معايير التشغيل المختلفة لتحسين جودة الاتصال. هناك حاجة إلى تنفيذ طبقة مادية مرنة وقابلة للتكيف لتحقيق افضل نظام راديو ادراكي .

في هذه الرسالة ، يعتمد النظام المقترح على الاكثر فائدة من تقنيات لانتشار الطيف في شبكات الراديو الإدراكي استنادًا إلى المعلمات المستخدمة والمتمثل بطيف انتشار القفز الترددي (FHSS) لتلبية متطلبات الطبقة المادية داخل معمارية شبكة الراديو الادراكي. النظام المستخدم يعتمد على معاملات محاكاة الإنتاجية ومعدل انخفاض البيانات ووقت الكشف ووقت التأخير.

إلى جانب ذلك ، يحاكي النظام المقترح هجوم التشويش بالضوضاء في بيئة شبكة الراديو الادراكية. علاوة على ذلك ، تم تنفيذ النظام المقترح باستخدام أداة محاكاة OMNET ++. لذلك ، فإنه يحاكي نظام الأمان مع (6 CR أو مستخدمين ثانويين) تم تصنيفهم على أنهم وحدات عسكرية و (20 مستخدمًا أساسيًا) تم وضعها كوحدات GSM ذات نطاق تردد مرًخص.

محاكاة هجوم التشويش بالضوضاء في بيئة CRNs في جميع دراسات الحالة حيث يعرض النظام المستخدم تأثيرات هجوم الضوضاء والتشويش من خلال تقليل الإنتاجية وزيادة معدل إسقاط البيانات ووقت الكشف ووقت التأخير.

تظهر نتائج حالة محاكاة CR أن دراسة حالة FHSS أفضل من دراسة الحالة لـ RSA و RSA-FHSS اعتمادًا على معلمات المحاكاة مثل الإنتاجية ومعدل انخفاض البيانات ووقت الكشف ووقت التأخير.

في حين أن أفضل دراسة حالة مستخدمة للتخفيف من هجوم التشويش بالضوضاء هي النظام المركب المستند إلى دراسة حالة RSA-FHSS.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل

تحسين أمنية شبكة الراديو الادراكية بالاعتماد على RSA وتقنية القفز الترددي

رسالة

مقدمة إلى مجلس كلية تكنولوجيا المعلومات في جامعة بابل والتي هي جزء من متطلبات الحصول على درجة الماجستير في تكنولوجيا المعلومات – شبكات المعلومات

اوس احمد كاظم

باشراف
أ.د ستار بدر سدخان

هـ 1442 م 2021

الخلاصة