Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
Information Technology
Department of Information Networks

EFFICIENT PRIMARY USER ALLOCATION IN SECURE COGNITIVE RADIO ENVIRONMENTAL APPLICATION

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.

By

Zamzam Ali Abood Noory

Supervised by

Prof.Dr. Sattar B. Sadkhan

2023 A.D. **1445 A.H**

بسم الله الرحمن الرحيم

يرفع الله الذين آمنوا منكم
والذين أوتوا العلم درجات والله
بما تعملون خبير

صدق الله العظيم

سورة المجادلة . آية 11

Certification of the Examination Committee

We hereby certify that we have studied the thesis entitled (**EFFICIENT PRIMARY USER ALLOCATION IN SECURE COGNITIVE RADIO ENVIRONMENTAL APPLICATION**) and examined her in its content and what is related to it, and that, in our opinion, it is adequate with (**Very Good**) standing as a thesis for the degree of Master in Information Technology-Information Networks.

Signature:
Name: Hadi T. Ziboon
Title: Prof. Dr.
Date: / / 2023
(**Chairman**)

Signature:
Name: Mohammad Hussein Jawwad
Title: Asst. Prof. Dr.
Date: / / 2023
(**Member**)

Signature:
Name: Tariq Alwan Kadhum
Title: Lecturer
Date: / / 2023
(**Member**)

Signature:
Name: Sattar B. Sadkhan
Title: Prof. Dr.
Date: / / 2023
(**Member and Supervisor**)

Approved by the Dean of the College of Information Technology, University of Babylon.

Signature:
Name: Prof. Dr. Wesam S. Bhaya
Title: Professor
Date: / / 2023
(**Dean of Collage of Information Technology**)

Supervisor Certification

I certify that the thesis entitled (**EFFICIENT PRIMARY USER ALLOCATION IN SECURE COGNITIVE RADIO ENVIRONMENTAL APPLICATION**) 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: / /2023

The Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled "**EFFICIENT PRIMARY USER ALLOCATION IN SECURE COGNITIVE RADIO ENVIRONMENTAL APPLICATION"** for debate by the examination committee.

Signature:

Asst. Prof. Dr. Alharith A. Abdullah

Head of Information Networks Department

Date: / /2023

Declaration

I hereby declare that this thesis, 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 : **Zamzam Ali Abood Noory**

Date: **/ / 2023**

Dedication

I dedicate this thesis

To the soul of my father

To the fountain of patience my mother

To my supervisor

To my family

To my friends

Researcher

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 their 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.

Sincere appreciation and love go to my family, my father's soul who he was always be with me in my heart 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

Researcher

Abstract

Cognitive Radio Network (CRN) is an important technology due to its capacity to solve the issue between the restricted spectrum supply and spectrum demand from the growing wireless applications and services. however, due to the nature of these networks, CRNs are exposed to different types of threats and attacks from different malicious users, which can affect the network availability and performance. The proposed system is based on enhancement security of cognitive radio network for the environment application, using two secure methods: the first method is the (Advanced Encryption Standard (AES), Rivest Cipher (RC-5) encryption algorithms as the data message in OMNET++ and channel allocation with fuzzy logic method, the second method is cognitive trusted party (CTP) approach to provide integrity with Secure Hash Algorithm Version 3 (SHA-3) and authentication with Elliptic Curve Cryptography (ECC).

The best performance of the 1st security system is measured by the total average throughput of sent packets of 4 SUs and 10 PUs is 4.7 Bps, 8 SUs; of 20 PUs is 8.9 Bps; of 16 SUs and 30 PUs is 7.2 Bps. Fuzzy Logic channel enhancement with 16 SUs and 30 PUs is 7.8125 Bps.

The best performance of the 2nd security system is calculated with the total average probability of channel collision of the ECC case as 0.0723; SHA-3 case as 0.0568; and of ECC with SHA3 case as 0.0516. The total average Packet Delivery Ratio (PDR) of the ECC case is 99.17 %; the SHA-3 case is 0.99.71 %, and the integrated system of the ECC with the SHA3 case is 99.84 %. The best results without security compared with related works as Fuzzy Logic resource allocation the PDR is 98.71 % and the Packet Drop rate is 10 %.

Table of Contents

Table of Contents

CHAPTER THREE THE PROPOSED APPROACH

Table of Contents

List of Tables

Chapter 2

Chapter 4

List of Figures

List of Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
AMC	Adaptive Modulation/Coding
AOA	Angle of Arrival
BSs / APs	Base Station / Access Point
Bi-PUF	Binate physically Unclonable Function
BAN	Body Area Network
CE	Cognitive Engine
CR	cognitive Radio
CRNs	Cognitive Radio Networks
CTP	Cognitive Trusted Party
CCSD	Control Channel Saturation DoS Attack
COOPON	Cooperative Neighbouring Cognitive Radio Nodes
CSS	cooperative spectrum sensing
DSA	Digital Signature Algorithm
DoA	Direction of Arrival
ECC	Elliptic Curve Cryptography
EED	End-to-End Delay
FK-means	feature-based K-means
FB	Frequency band
HRA-SKC	Hybrid Routing Algorithm - Symmetric Key Cryptography method
IoT	Internet of Things
MUs	Malicious Users
MS	Mobile Station
NAN	neighborhood area network
NS-2	Network Simulator
OMNET ++	Objective Modular Network Testbed in C++
OMTriO-CFO	one-to-many matching-based TriO-CFO algorithm
PU	Primary User
PU-BS	Primary user base station
PUE	Primary User Emulation
PKCS	Public-Key Cryptography Standards
QoS	Quality of service
RSS	Received Signal Strength
RC5	Rivest Cipher

RSA	Rivest–Shamir–Adleman
SUs	secondary users
SHA-1	Secure Hash Algorithm -1
SSL	Secure sockets layer
SCN	Selfish Channel Negotiation
SNR	Signal-to-noise ratio
SSDF	Spectrum Sensing Data Falsification
TKIP	temporal key integrity protocol
TTP	Third Trust Party
TA-FuReil	Topology aware fuzzy-reinforcement learning
TCP/IP	Transmission Control Protocol/Internet Protocol
TPC	Transmit power control
TLS	Transport Layer Security
UWB	ultra wide band
WEP	wired equivalent privacy
WLANs	wireless local area networks
AMC	Adaptive modulation/coding
AOA	Angle of Arrival

List of Thesis Related Publications

1st paper Name of Conference:

- **2022 5th International Conference on Engineering Technology and its Applications (IICETA).**

Title:

- **Security evaluation techniques of Cognitive Radio Network status and challenges.**

Published Link:

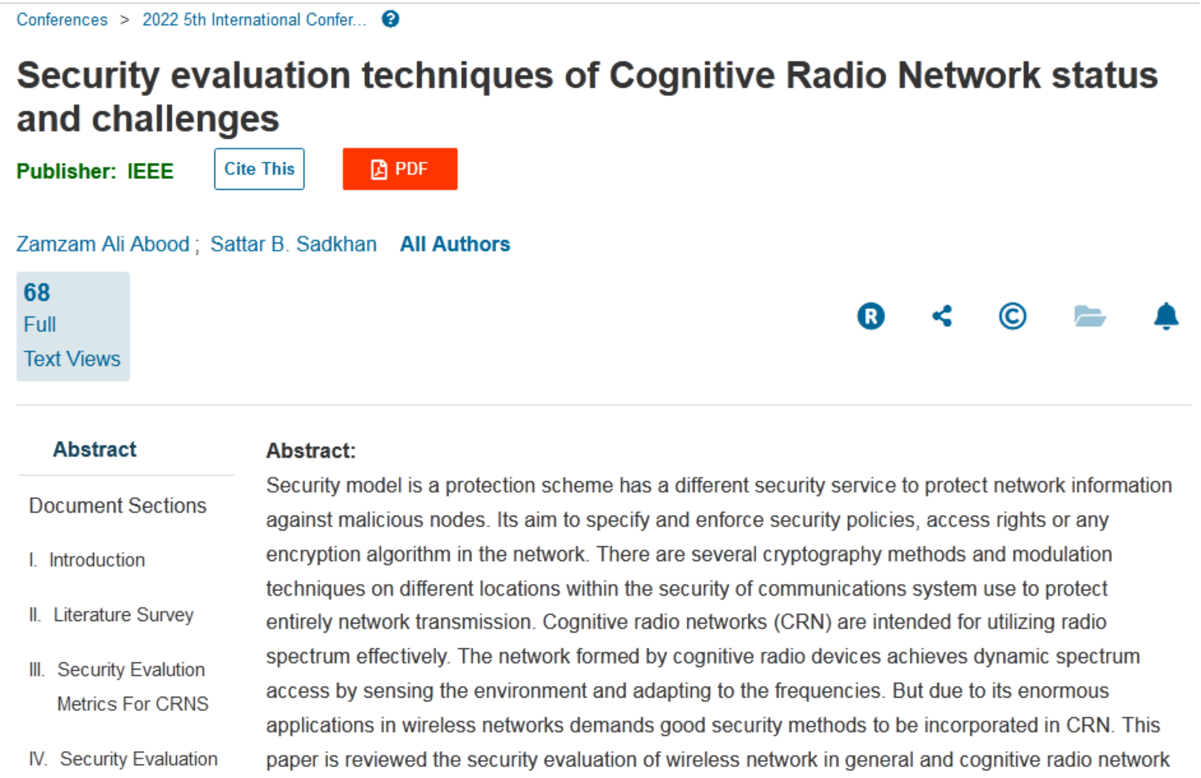
https://ieeexplore.ieee.org/document/9888422

- **Authors:**
  - Zamzam Ali Abood
  - Prof.Dr. Sattar B. Sadkhan

Information Network Department, Information Technology College, Babylon University.

Email: zmzmasas97961328@gmail.com

Email: drengsattar@gmail.com



Conferences > 2022 5th International Confer...

Security evaluation techniques of Cognitive Radio Network status and challenges

Publisher: IEEE

Cite This

PDF

Zamzam Ali Abood ; Sattar B. Sadkhan All Authors

68
Full
Text Views

Abstract

Document Sections

Abstract:

Security model is a protection scheme has a different security service to protect network information against malicious nodes. Its aim to specify and enforce security policies, access rights or any encryption algorithm in the network. There are several cryptography methods and modulation techniques on different locations within the security of communications system use to protect entirely network transmission. Cognitive radio networks (CRN) are intended for utilizing radio spectrum effectively. The network formed by cognitive radio devices achieves dynamic spectrum access by sensing the environment and adapting to the frequencies. But due to its enormous applications in wireless networks demands good security methods to be incorporated in CRN. This paper is reviewed the security evaluation of wireless network in general and cognitive radio network

Chapter One

General Introduction

1.1 Introduction

Wireless technologies, applications and services have been witnessed a rapid growth in the past few years, due to this development, spectrum scarcity and shortage has become a major concern, several spectrum portions of the static allocated licensed bands are under-utilized. Cognitive radio networks (CRNs) are considered to be the most promising solution in improving the spectrum utilization and solving the spectrum scarcity by providing licensed spectrum portions to unlicensed users, however due to nature of these networks, CRNs are exposed to different types of threats and attacks from different malicious users, which can affect the network availability and performance [1].

Radio spectrum is a significant and inherent asset employed in wireless communication services and applications, due to the rapid growth of wireless licensed users subsequently applications and services would demand a huge radio spectrum, resulting in constraints and insufficiency due to inflexible allocation policies. Underutilization issue in radio spectrum has been tackled through the development of a CR system. This intelligent radio system enables opportunistic spectrum access, thereby resolving the problem of radio spectrum scarcity and shortage. The proposed approach entails enabling SUs to utilize licensed radio spectrum gaps or white spaces in an opportunistic manner, while ensuring that no interference is caused to primary user [2].

Due to the intelligence and nature of CRNs, they are vulnerable to serious security attacks and threats from many malicious and selfish users that selfishly exploit the legitimate spectrum to their own interest and cause interference PUs compared to traditional wireless networks, that could affect the network performance, so security concerns are further escalated to the forefront and have taken on an increasingly important role in CRNs [3]. The interference caused by such malicious users can have a detrimental effect on the network performance, thereby exacerbating security concerns. Consequently, security has become a critical consideration in CRNs and has assumed an increasingly significant role. Hence, it is necessary to ensure the authentication of entities and data, particularly the Secondary Users (SUs) within Cognitive Radio Networks (CRNs), and to attain data integrity and non-repudiation, as well as other fundamental security requisites, in order to safeguard CRNs against established forms of attacks [4].

There are different cryptosystem used to secure cognitive radio networks data transmission as follows:

- Symmetric encryption: It is basic form of encryption that utilizes a single secret key for both encryption and decryption of information. It employs a confidential key, which may take the form of a numerical value, a lexical item, or a sequence of arbitrary characters. Text manipulation refers to the process of modifying the content of a message by blending plain text in a specific manner. An example of Symmetric encryption algorithms are Blowfish, AES, RC4, DES, RC5, and RC6. AES is the most commonly utilized, it has a three key lengths: AES-128, AES-192, and AES-256. A primary limitation of symmetric key encryption is the requirement for all parties to exchange the encryption key prior to decryption of the data. As represented in Figure 1.1 [5].

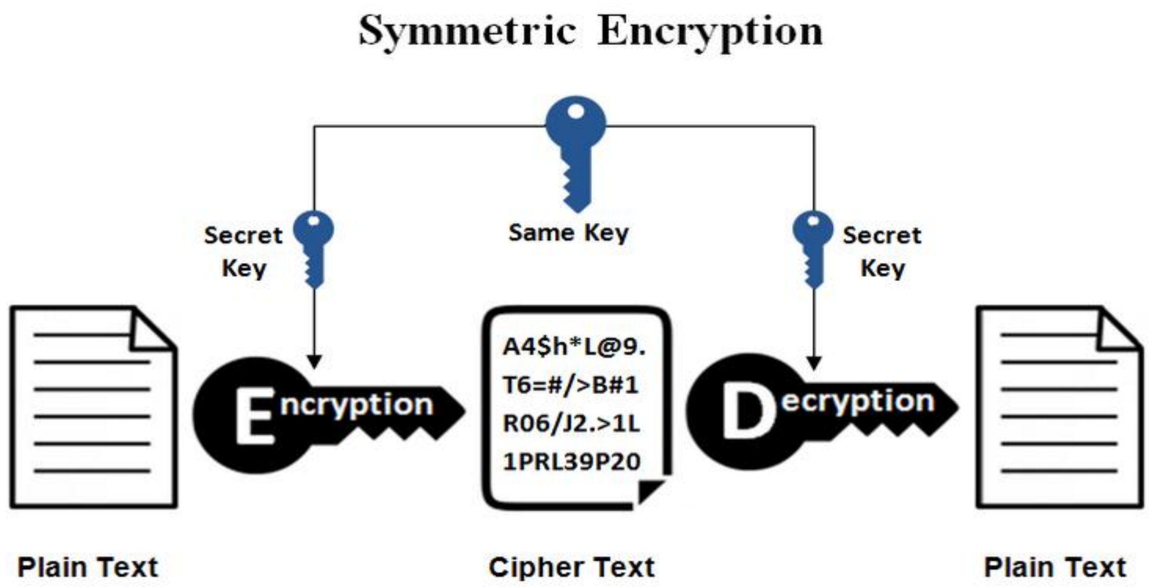


Figure 1.1: Symmetric Encryption [5].

- Public key cryptography (Asymmetric encryption) : It is a comparatively recent technique in contrast to symmetric encryption. It employs a pair of distinct keys to encode a plaintext. The exchange of secret keys occurs through the utilization of the Internet or a vast network. The purpose of this measure is to prevent unauthorized individuals from exploiting the keys for malicious purposes. It is noteworthy that the possession of a secret key enables an individual to decipher the message, thereby underscoring the significance of utilizing two interrelated keys in asymmetric encryption to enhance security. The public key is openly accessible to any potential sender who wishes to transmit a message to the intended recipient. The second private key is maintained in confidentiality to restrict access exclusively to authorized parties [6].

It implemented in contemporary communication channels, particularly those that operate through the Internet. An example of

Asymmetric key encryption algorithms are RSA, DSA, Elliptic curve techniques, and Public-Key Cryptography Standards (PKCS). Figure (1.2) illustrates asymmetric key encryption algorithms [7].

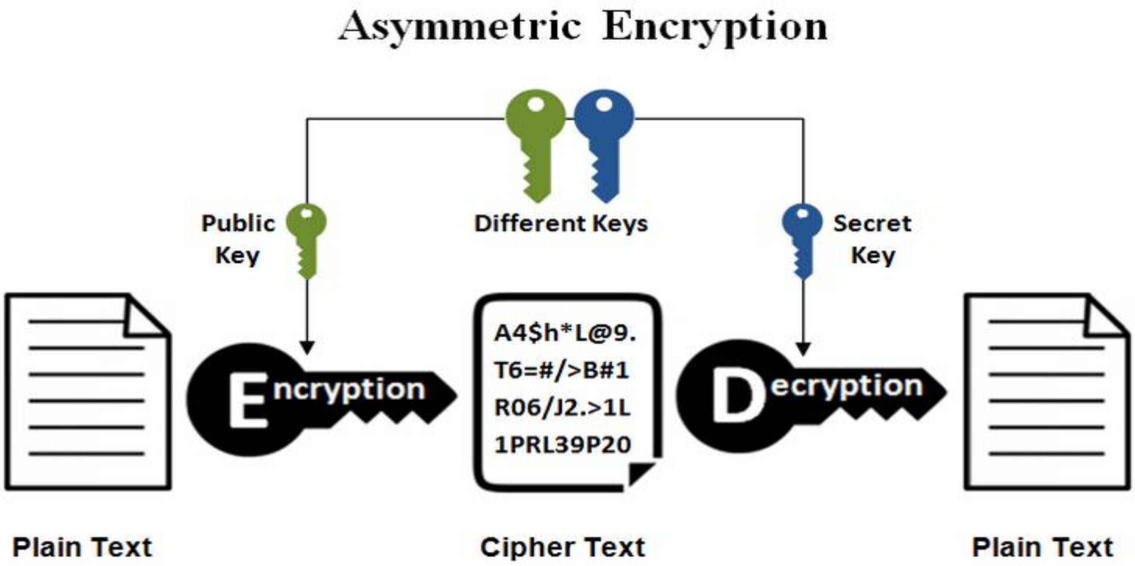


Figure 1.2: Asymmetric Encryption [7].

Moreover, various encryption techniques are employed in diverse wireless network the susceptibility of CRNs to security breaches and risks posed by malevolent users who manipulate the authorized spectrum for their own benefit is a widely acknowledged concern [8].

Cognitive radio technology holds the potential to enable radios with advanced cognitive capabilities that can obtain knowledge and dynamically adjust their behavior in response to changes in their surrounding environment. The vacant frequency bands, also known as spectrum gaps or white spaces, are depicted in Figure 1.3 [9].

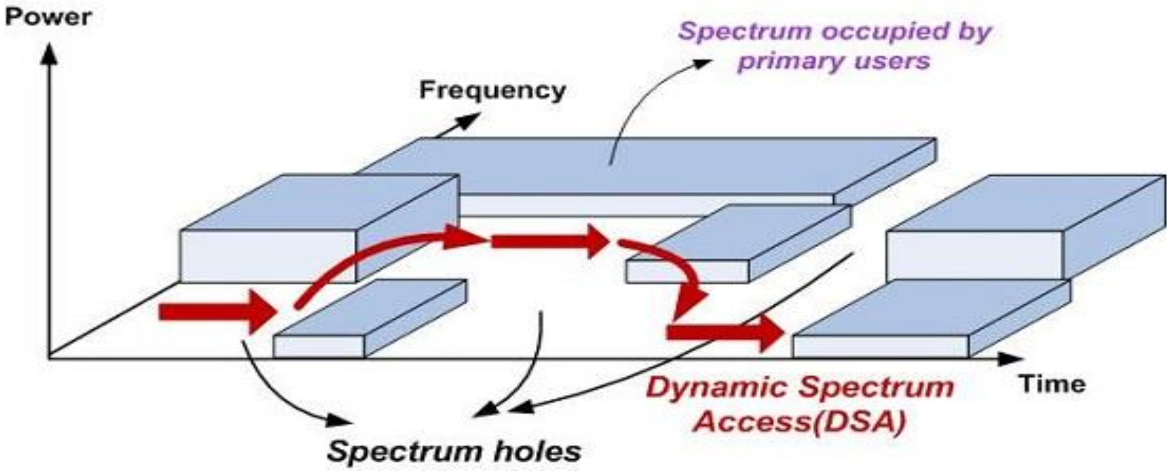

Power
Frequency
Spectrum occupied by primary users
Time
Dynamic Spectrum Access(DSA)
Spectrum holes

Figure 1.3: cognitive radio spectrum gaps [9].

The main consideration in the context of CR systems is security. The system is designed to conform to security parameters and techniques that align with the objectives set up by the system administrator. During the initial phase, the establishment of network security policies enables the system to operate autonomously and attain the required level of security. It mitigates security risks that may arise from human error or inadvertence. The automated methodology utilized by CR efficiently handles security parameters, amplifies situational awareness, and protects the crucial network. Nonetheless, further measures are required to fortify protection against contemporary threats [10].

1.2 Related Work

Various relevant studies have been compiled and synthesized under the umbrella of related works.

An evaluation of security breaches targeting spectrum sensing in CRN was performed by Mapunya et al. The process of spectrum sensing is an essential element within the cognitive cycle of a cognitive radio network (CRN). Nonetheless, any compromise in this phase can have adverse effects on the overall functionality of the cognitive network. The SSDF attack poses a significant security challenge to CRN, particularly those that employ CSS techniques. It was demonstrated that incorporating CSS as a sensing mechanism can improve the ability to detect primary users in situations where secondary users are sharing sensing data. The SSDF attack had a detrimental impact on the performance of CRNs, leading to suboptimal utilization of the available spectrum resources. The efficacy of the COOPON and Pinokio schemes was evaluated within a simulated setting. The results showed that the COOPON initiative is efficacious in mitigating the influence of malicious actors [11].

A study detection scheme is proposed by Develi et al. that spectrum sensing entailed two stages and employs fuzzy logic . The initial phase entails the implementation of a dynamic dual-threshold energy detector, succeeded by the application of a fuzzy logic system in the ensuing phase. The scheme was analyzed in the context of cooperative sensing, demonstrating significantly better performance compared to conventional collaborative spectrum-sensing schemes. The results showed superior effectiveness when compared to traditional two-stage identification methodologies [12].

The utilization of the Fuzzy Logic System was employed by Aksatha et al. to enhance Quality of Service in information transmission, thereby amplifying energy efficiency. The selection of the optimal channel for transmitting a signal in a given space-time was based on the criterion of achieving the highest possible immediate achievable rate. The concept of QoS can be deconstructed, and monitoring bandwidth has been found to enhance various performance metrics, including Total Consumed Energy, Total Remaining Energy, Packet Delivery Ratio, Throughput, and Energy Lifetime. The employment of the Fuzzy logic framework represented a noteworthy application in the utilization of energy. The results showed previous approaches demonstrated progress in terms of energy amplification and complexity[13].

A reliable method of detecting available radio frequencies in cognitive radio networks is proposed by Chakraborty et al. A fuzzy logic-based selection method was suggested for the identification of the most suitable secondary users in Multi-user cooperative cognitive radio systems as a type of communication network that utilizes cognitive radio technology to enable multiple users to share the available spectrum resources in a collaborative manner. It involved the integration of three discrete input variables, namely Signal-to-Noise Ratio (SNR), Channel Quality, and Trust Factor, in a joint manner to select eligible SUs. The results showed enhanced efficacy in detecting and removing Malicious Users (MUs) and decrease in the likelihood of missed detection by excluding MUs from the decision-making process [14].

The utilization of dynamic cluster switching is proposed by Monisha et al. to address the challenge of secure channel allocation in cognitive radio. It is based on a novel methodology for ensuring secure channel allocation in smart grid communications that employ cognitive radio technology. SCAN-CogRSG, utilized dynamic cluster switching. The Bi-PUF authentication mechanism was employed to facilitate resilient authentication for secondary users (SUs). The utilization of the FK-Means algorithm and the TriO-CFO algorithm was proposed of achieving efficient channel allocation. The results showed an improvement in throughput, retransmission, latency, and duration of authentication [15].

A novel clustering protocol is proposed by Ponnrajakumari et al. for cognitive radio networks that prioritizes security and reliability. The utilized methodology involved the application of fuzzy clustering and optimization techniques based on the Fibonacci sequence and the golden ratio. The results showed that the clustering method proposed is effective in achieving a high level of clustering efficiency and the formation of clusters that are free from attackers, when compared to other studies that are relevant [16].

A novel approach is presented by Sasipriya et al. that could achieve optimal performance by utilizing a fuzzy-based clustered greedy algorithm. This method effectively mitigated the risk of interference in primary user confidentiality. It involved a thorough assessment of the impact of both injection and reactive jamming attacks on the wireless communication phase. The utilization of convolutional neural networks had the potential to facilitate the detection and differentiation of various types of attacks. The simulation results of resource allocation algorithm not only facilitated the acquisition of transmission opportunities for secondary users (SUs), but also enhanced the efficacy of primary user (PU) security in the face of unforeseen attacks [17].

A fuzzy inference system is proposed by Nassef et al. that relied on four descriptors that were in conflict with one another. A model of attack has been developed with the aim of assessing the likelihood of detecting secondary users, both honest node and malicious node. The results showed that the integration of reputation sensing into the fusion center has resulted in improved precision in detecting spectrum and effectively deterred malevolent secondary users from engaging in the fusion process of spectrum detection [18].

Secure SHA-1 with a neural network is proposed by VasanthaReddy et al. which is a form of soft computing, in order to prevent primary user emulation attacks. The localization between primary and secondary users was achieved through utilization of RSS and DoA. The primary aim of the proposed methodology was to reduce the loss ratio that occurs during the process of communication. The evaluation of the RSS-DoA-SHA technique was conducted with regards to routing overhead, EED, and loss ratio. The performance of the RSS-DoA-SHA method was assessed in comparison to two established methods, namely the AOA method and the HRA-SKC method. The proposed method exhibited a lower end-to-end delay of 1ms for 500 processing units, in contrast to the RSS-AOA method [19].

An enhanced method is proposed by by Lafia et al. for identifying PUE attacks within CRNs. A model based on hybrid signal processing of free space path loss and additive Gaussian noise. The detection of the transmitter's position was accomplished through implementation of the free space path loss model. The simulation results indicate that the suggested model has enhanced precision in identifying primary user emulation attacks. It is finding indicated that the hybrid model proposed as capable of detecting PUE assaults in CRNs, while considering the number of secondary users and the speed of the transmitter [20].

1.3 Problem Definition

CRNs are susceptible to a range of threats and attacks perpetrated by malicious users, which can have detrimental effects on network availability, performance, authentication, integrity, and non-repudiation of services. Therefore, it is an important to implement an effective security system to mitigate and eliminate attacks to the greatest extent possible.

- There are different security issues of network intrusions states due to the security gab in the nature of wireless cognitive radio network for example detecting layers and cross-layers attacks in CRNs.
- So the main problem is : How to find suitable security system and evaluation method to evaluate and to test a secure CRNs environment.

1.4 Thesis Contribution

The main contributions are represented by :

- Efficient data transmission to enhance the security limitation for data transmission because of the security increase size of data packets after encryption and this make network effect and throughput is decreased.
- Improvement of delay due to the security system by channel resource allocation for customized a fuzzy logic approach as it managed performing channel selection, channel switching, and spectrum allocation in CRN, it enhanced decision making in cognitive radio network.
- Clarify the security aspects and proofs for the proposed model (Digital signature of SHA-3, and public key authentication of ECC) against layered well-known attacks.

1.5 Aims of the Thesis

The aim of the proposed system is to developed security evaluation techniques for wireless cognitive radio networks by implementing two security systems with AES, and RC5, ECC, and SHA-3 by:

- Designing and testing a customized digital signature scheme with SHA-3, and ECC authentication method as an integration method to provide data integrity and authentication in CRNs.
- Establishing a process to continuously evaluate and strengthen security systems and processes.
- Evaluating the proposed crypto system with the SHA-3 and ECC methods.
- Increasing packet delivery ratio through increasing total acknowledged packets which arrived without errors.
- Decreasing probability of channel collision of primary users through authentication phase by CTP, and primary user base-station.

1.6 Thesis Outline

Thesis outline is structured as follows:

Chapter Two: This Chapter provides a theoretical background for this work.

Chapter Three: It shows the adopted methodology to meet the research objectives and the main structure of the proposed system. This encompasses the main functionalities that the system can perform.

Chapter Four: This Chapter depicts the designed system and its main features that can be used by different types of users.

Chapter Five: In this Chapter, a conclusion about this work and possible future research directions will be provided.

Chapter Two

Theoretical Background

2.1 Introduction

Initially, the implementation of fixed spectrum assignment policies in wireless applications results in a considerable depletion of valuable spectrum resources, ultimately leading to spectrum scarcity. Mitola's Cognitive Radio Technology utilizes an automated detection method based on Dynamic Spectrum Access to efficiently leverage the untapped channels within the wireless spectrum band [21]. The categorization of cognitive radio systems be broadly divided into three main paradigms [22].

- **The underlay paradigm:** 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 example,Ultra-wideband (UWB) communications. Besides, it's also be used in the field of the unlicensed spectrum bands to produce different user services [23].
- **The overlay paradigm:** The transmitter of SU identifies the channels furthermore, the messages with codebooks of the PU. It is transmitted simultaneously with PU, as long as the interference is decreased by some collaboration, for example via the concept of relaying (FB) [24].
- **The Interweave 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]. This is an important point to clarify that the is used system based on the third paradigm (Interweave Paradigm) [25].

The three main cognitive radio paradigms are shown in Figure 2.1 [25].

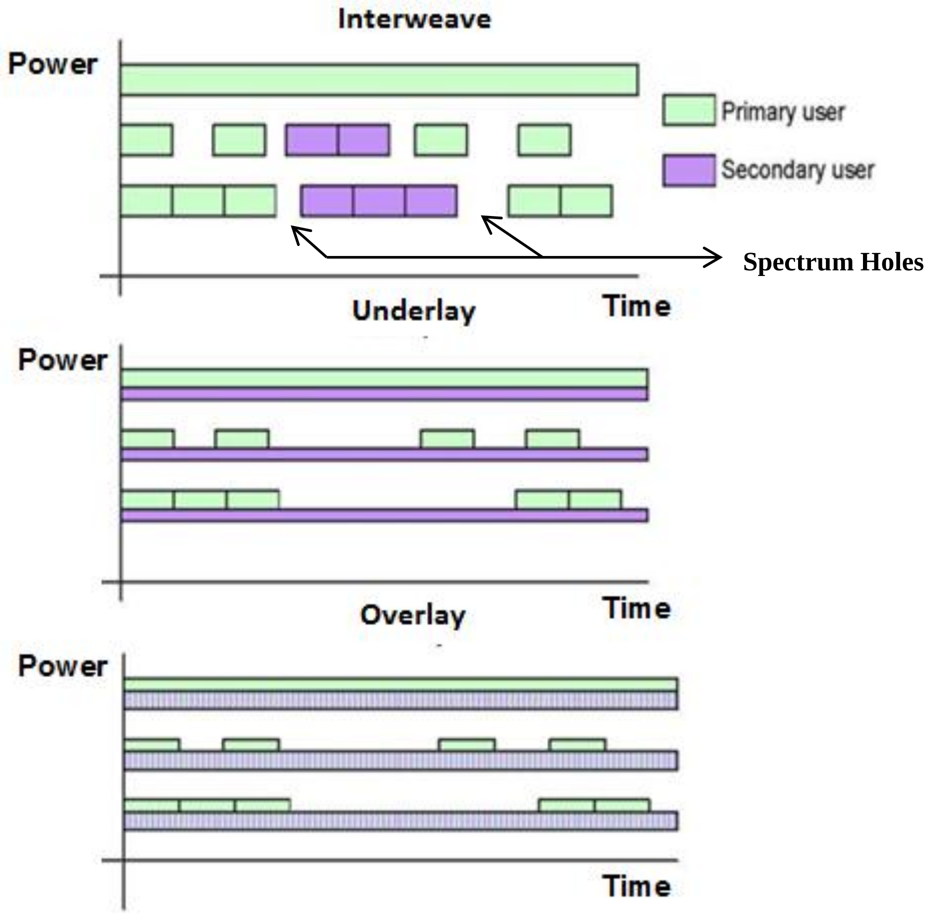


Figure 2.1 : cognitive radio paradigms [25].

CR nodes are categorized according to their cognitive functionality as determined by the cognitive cycle. In cases where a collection of environmental parameters are present, the system possesses the capability to self-organize and adapt to reconfigure itself in a highly flexible and transparent manner [26].

The concept of cognitive ability can be concisely summarized as follows:

- **Spectrum sensing** : It is related to the ability of a CR Node to identify vacant portions of the frequency band allocated for communication purposes, while ensuring minimal interference with primary users, as previously outlined. The acquired information is then shared with neighboring nodes [26].

- **Location identification** : It refers to the cognitive node's capacity to determine its own location and that of other transmitter nodes within the network. There exist various methodologies and frameworks for acquiring location-based data, encompassing both manual approaches and reliance on external systems such as extended geographical location systems [27].
- **Network/system discovery**: Naturally, so that the cognitive node can achieve the best way to communicate and share network characteristics it must firstly, discover the networks which is available within the coverage area [28].
- **Service discovery** : after the network discovered and connected within the network, it's possible to get the network services, so this feature is linked to network discovery capability and then the possibility of finding the appropriate service suited to the node requirements [29].
- ***Reconfigurable Capability*** : the ability of the cognitive node to reconfigure itself. Consequently, the characteristic is described in the following points [30]:
- **Frequency agility**: It pertains to the capacity of a CR node to adaptively adjust its operational frequency parameters to choose the most suitable frequency, taking into account the signal awareness of other transmitting devices [30].
- **Adaptive modulation/coding (AMC)** : it developed as an approach channel capacity in the Fading Channels . Where the ability of the CR node to modify the characteristics of the transmitter to improve access to the spectrum and its optimal use by choosing the best modulation type for use, however, to support systems compatibility [30].

- **Transmit power control (TPC)**: It is a mechanism that facilitates dynamic modification of transmission power levels during data transmission. This mechanism employs a selective approach to effectively reduce power levels [31].
- **Dynamic system/network access** : it's very important to work in Heterogeneous Wireless Networks environment, thus CR reconfigure itself to run different protocols that required to access the multiple Communication Systems/Networks [31].
- **Self-organized capability** : It exhibits a high level of intelligence in communication and compatibility with devices, which is attributed to its self-organized capability and other aforementioned characteristics. At this stage, the CR node is characterized by a unique set of attributes, which comprise spectrum/radio resource managing, mobility and connection managing, and trust/security managing, with the objective of enhancing network efficiency [32].

2.2 The Cognitive Radio Network

CRNs have been developed with the aim of enhancing spectrum access efficiency. Notwithstanding, these networks are susceptible to diverse forms of attacks and failures that have the potential to jeopardize the security and efficiency of their users [33].

2.2.1 Benefits of Cognitive Radio Network

- Greater flexibility compared with traditional wireless network and it was developed to enhance spectrum availability within wireless networks [34].
- The CRN integration with sensor networks, aspects of mobility, geo-routing, applications for healthcare, vehicular sensor systems.

- Dynamic spectrum access refers to the ability of wireless devices to access and utilize available radio frequency spectrum in a flexible and adaptable manner.
- Self-organizing networks : It has the ability to autonomously configure and optimize themselves without the need for external intervention.
- The security aim is to reduce the impact of interference through the implementation of cognitive anti-jamming systems.
- The utilization of a CE based SDR techniques to improve QoS, multi-band and multimode operation, and low-cost features to ensure interoperability with SDR technology [35].
- The utilization of wireless sensor network and IoT applications has been found to significantly enhanced the device lifetime in secure system [36].
- Improving energy efficiency and throughput in secure CRN-WSNs [37].

2.2.2 Disadvantages of Cognitive Radio Networks

- The issue of updated sensing information, due to channel failure and receiver uncertainty, which can effect on decision-making processes [38].
- The utilization of matched filtering feature in operations necessitates prior knowledge of the primary user in tactical settings [39].
- The interference of the channel is significant due to the wireless medium's nature as high sensitivity medium [40].

2.2.3 Challenges of Cognitive Radio Networks

- The decision-making approaches utilized in the context of cognitive radio spectrum sensing [42].
- Multi-hop routing of intelligent jamming-aware techniques [43].

- Detecting cyberattacks and fraud [44].
- Cooperative Spectrum Sensing of the hidden terminal and the ensuing complexity [45].
- The sensitivity of detection within a spectrum of broad frequency range [46].

2.3 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 [47]. The fundamental components of the CRN are categorized as MS, BSs/APs, and Backbone/Core Networks. The fundamental components of four distinct architectures, namely Infrastructure, Ad-hoc, Mesh Architectures, and Customized Secure CRNs Architecture, are represented by : [48] .

2.3.1 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 [49]. Figure 2.2 shows the infrastructure architecture and how network elements connected with each other [50].

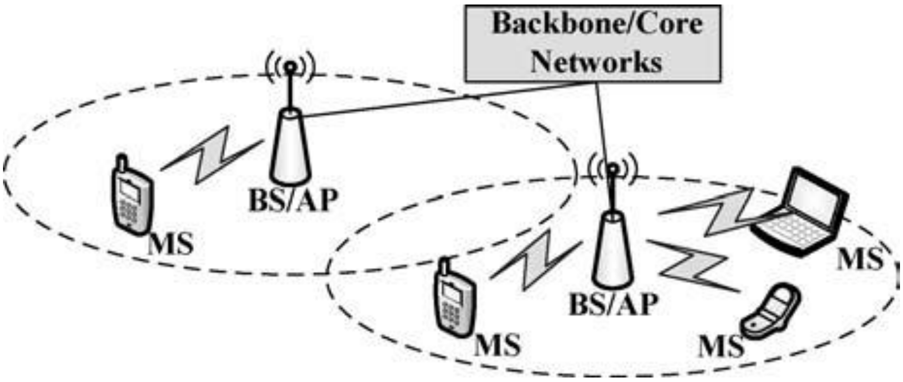


Figure 2.2: CRN Infrastructure architecture [50].

2.3.2 Ad-hoc Architecture

It is created without the need to rely on the infrastructure provided by the network, but rather on its ability to be established dynamically on-demand [51]. 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 [52].

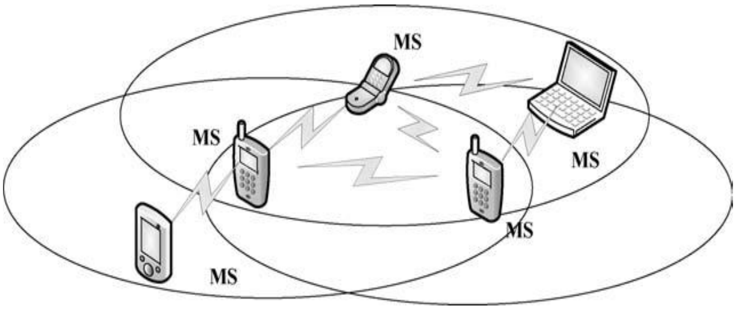


Figure 2.3: CRN Ad-hoc architecture [52].

2.3.3 Mesh Architecture

It integrates both previous types infrastructure and infrastructure-less (ad-hoc) architectures. Where the node within this architecture is directly connected to BSs / Aps or using another node MSs as multi-hop relay[53]. The architectural design of the CR-Mesh Network is shown in Figure 2.4 [54].

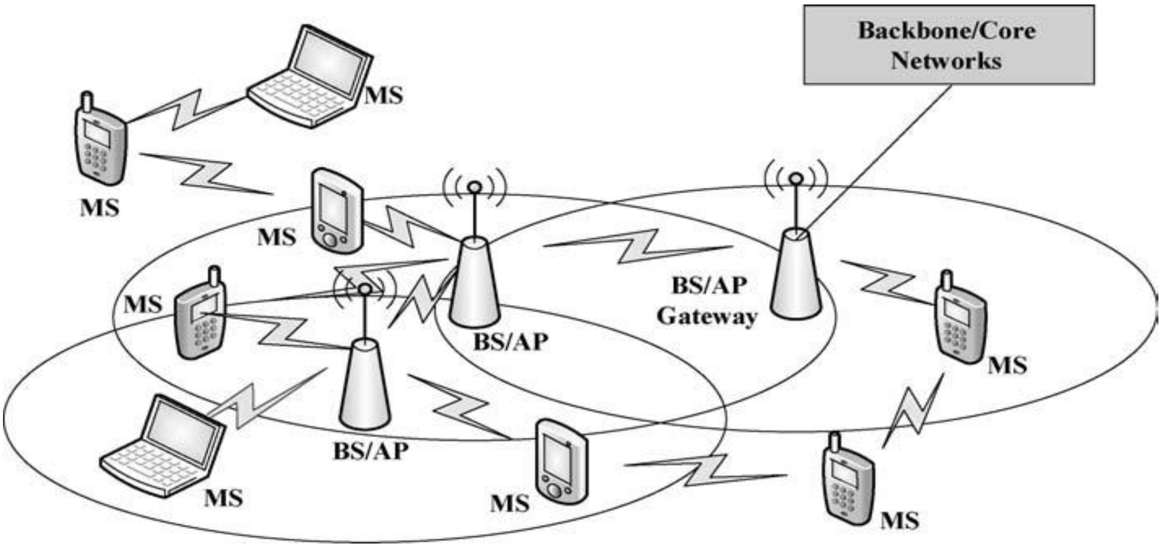


Figure 2.4: Architecture of a CR-mesh network [54].

2.3.4 Customized Secure CRNs Architecture

The CRNs can be categorized into two customized network elements. The first element is the primary network, comprises of PUs to provide the authorization to access a particular frequency band. The second network element is the cognitive network, consists of SUs which lack the privilege to access the spectrum [55]. In this architecture the network elements procedures is summarized as the following:

- PU own authorized access to the spectrum and is capable of accessing the channel at any given moment.
- The PU-BS is a type of base station that lacks sophisticated CR)capabilities. Its main function is to oversee the allocation and utilization of licensed spectrum for PUs [55].
- The Cognitive Radio User(SU), it has the complete capabilities, including the primary functions of the CR cycle. However, the SU is not licensed to access the spectrum and is therefore considered an unlicensed user [55].
- The Cognitive Radio Base Station or SU-BS is responsible for facilitating and managing the communication between CR users. It may get SSI either from a single, local CR user using spectrum sensing or from a group of CR users working together. In comparison to local spectrum sensing, the latter gives a more accurate evaluation of the current state of spectrum utilization [55].
- The TTP is responsible for furnishing nodes with both private and public keys, as well as generating key pairs through the utilization of the RSA public key cryptography algorithm [55].

2.4 Cognitive Radio Networks Applications

It has many applications in various fields, for instance, it can be used in places where the wireless sensor network(WSN) is used where CR developed as general technology within the applications of this network CR-WSNs, for example, Facility management, precision agriculture, machine surveillance, defensive maintenance, Medicine, telemetries, logistics, object tracking, intelligent roadside, safety, actuation and maintenance of complex systems, monitoring of the indoor and outdoor environment [56]

2.4.1 Leased Networks

In general, many cognitive radio network applications involve secondary users utilizing available resources in the absence of a primary user network, without providing any benefit to the primary user. In leased networks, the SU pays for itself to relay the PU's data transfer by leasing half of the time-slot from the PU. Figure 2.5 illustrates the leased network idea [56] .

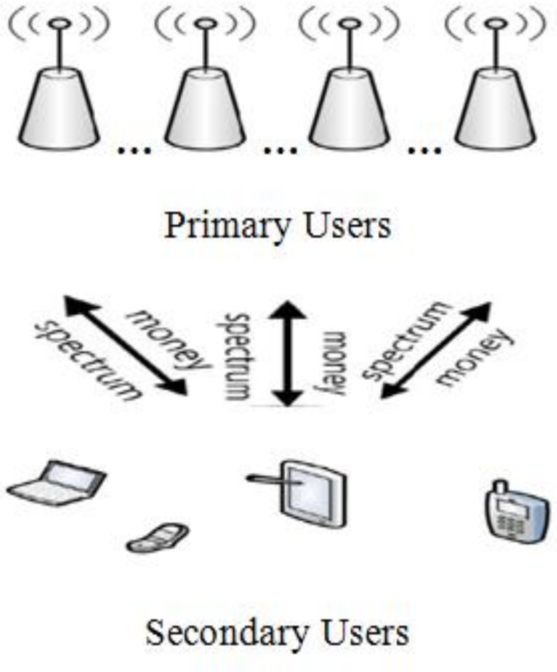


Figure 2.5: Leased Network concept [56].

2.4.2 Emergency Network

CRNs have the potential to serve as emergency networks, catering to critical services such as ambulance, fire, police, and rescue operations. It is necessary to allocate a significant amount of bandwidth, particularly in the event of natural disasters, as they can result in the collapse and failure of communication infrastructure [56].

Figure 2.6 shows how Cognitive Radio promotes quick rollout and unit-to-unit interoperability in networks in Disaster Relief environments, wherein communication units may be destroyed due to natural calamities such as earthquakes and floods. Such disasters may lead to the isolation of the affected area from other regions, thereby making it challenging to establish communication [56].

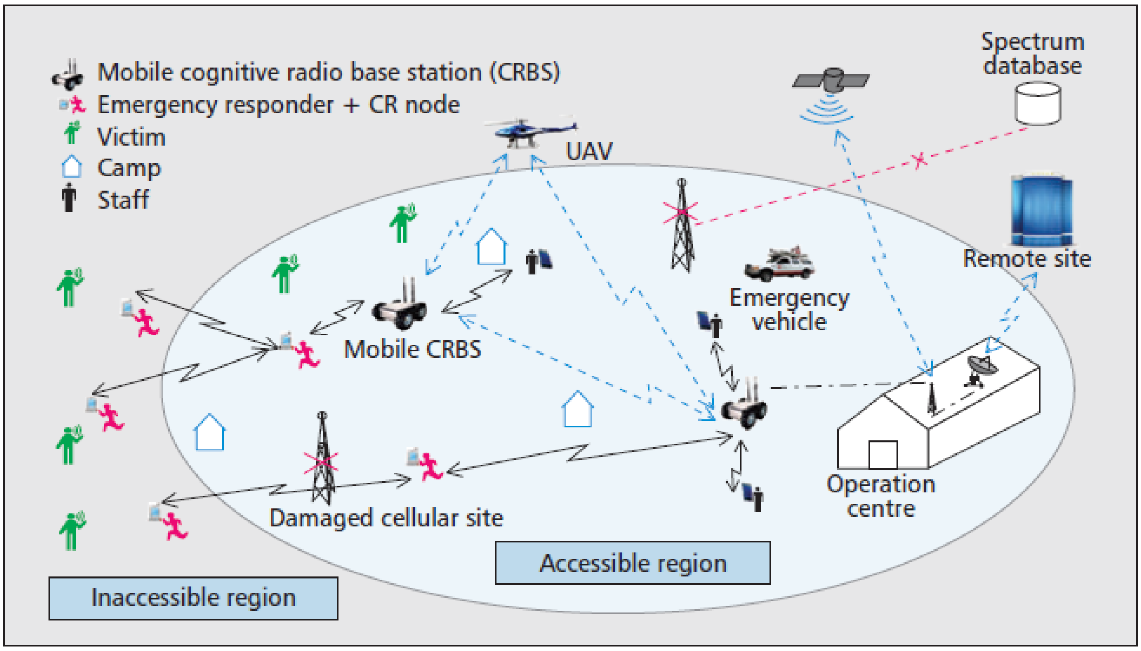


Figure 2.6: Emergency Network scenario [56].

2.4.3 Military Applications

Currently, ensuring secure communication in modern battlefields poses a greater challenge. Researchers prioritize security as the primary factor, followed by bandwidth [57].

Cognitive radio (CR) technology is represented in Figure 2.7, which includes spectrum awareness, cooperative sensing, rapid reaction time, and awareness and cooperation with other network resources. Furthermore, it is noteworthy that cognitive radio (CR) technology plays a crucial role in facilitating the collection of diverse wireless links from various military units, such as command, soldiers, satellite link, and UAV relay link networks [57].

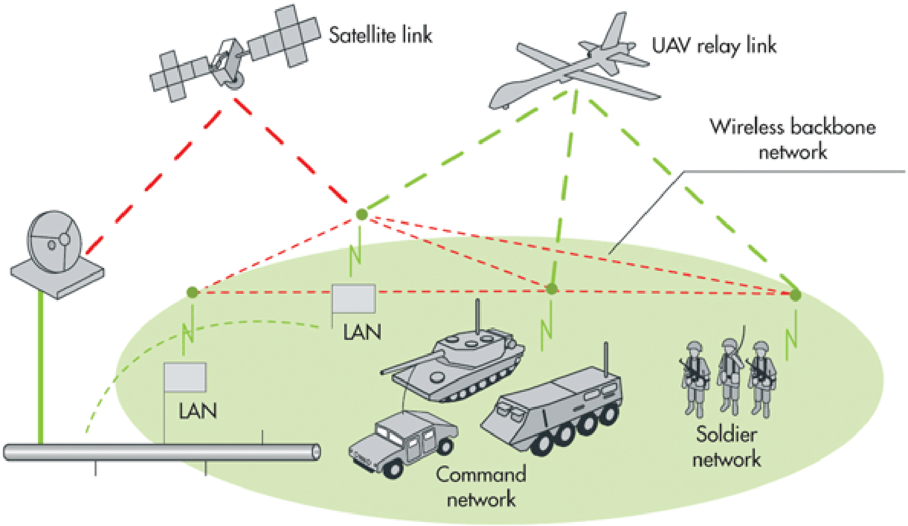


Figure 2.7: Intelligent a tactical Military network [57].

2.4.4 Healthcare Implementation

The medical data pertaining to human life is widely recognized as being of utmost importance and sensitivity. However, the conventional wireless sensor networks (WSNs) are limited to remote control, particularly in situations of congestion and overloading. The utilization of cognitive radio networks in this context has resulted in a high level of quality of service (QoS), as exemplified by its implementation in a Body Area Network (BAN), as depicted in Figure 2.8 [57].

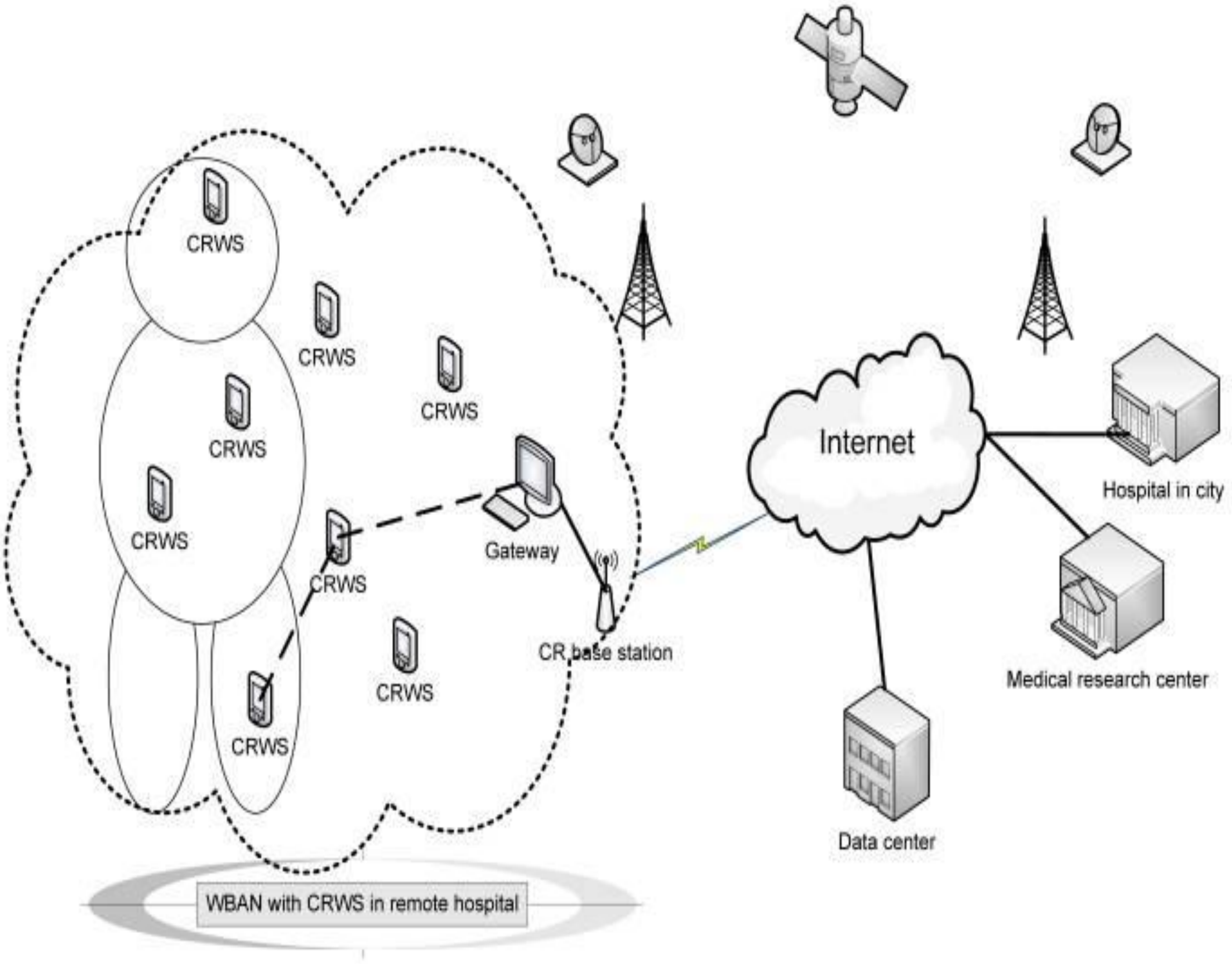


Figure 2.8 : Wireless Body Area Network (WBAN) with CR Wireless Sensor [57].

2.4.5 Transportation and Vehicular networking

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 [58].

As shown in the Figure 2.8, it links many vehicles and side and secondary roads that link the different methods of vehicles [58].

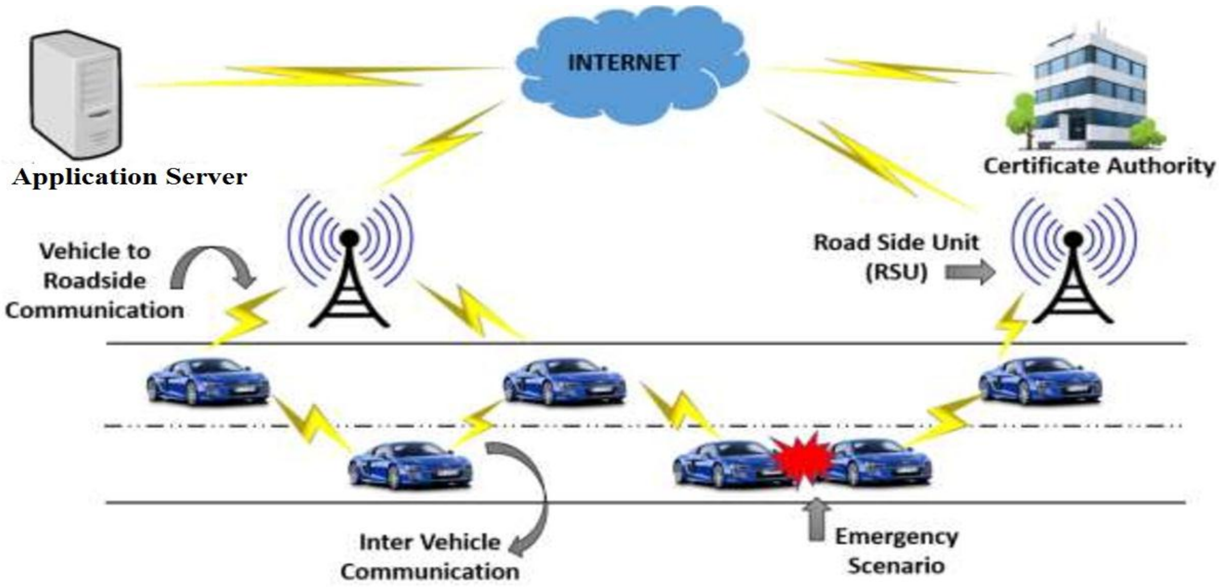


Figure 2.9: Transportation and Vehicular Networks [58]

2.5 Security of the CRNs

The cognitive radio network has garnered attention from researchers across various fields. Trends in research have focused on topics such as routing, spectrum radio sensing, and security threats. However, there is a need for increased attention to be given to the security of CRNs. The security measures implemented in cognitive radio networks. Security of CR networks is typically divided into two components. The first component is centered on preempting attacks, which is achieved through the use of cryptographic algorithms. The second component involves the detection of attacks, identification of malevolent behavior, and subsequent elimination of such behavior [58].

2.5.1 Security Benefits of CRNs

The development of various applications has been significantly motivated by the emergence of Cognitive Radio Networks (CRNs), particularly those that require reliable security measures to ensure effective decision-making with high levels of accuracy, safety, and real-time accessibility. This is particularly relevant in military applications, where network performance is of paramount importance. In this regard, CRNs have been instrumental in enhancing network performance through various means[59].

- Security
- The utilization of network resources
- The rate of adaptation
- The ability to interoperate

Safety is of utmost importance in this thesis. When it comes to safety, the CR system may adjust to whatever settings the admin decides are best, in accordance with network security policies during the preliminary phase. Subsequently, the system operates automatically to achieve the desired security level, thereby mitigating security threats that may arise from human intervention or unintentional actions. The CR system effectively manages security parameters, enhances situational awareness, and safeguards critical networks through automated means. However, in order to further fortify against contemporary threats, additional measures may be necessary [59].

2.5.2 Security Requirements for Cognitive Radio Networks

Cognitive radio networks, akin to various wireless networks, are susceptible to security concerns [60]. Furthermore, the wireless medium, being open-air, is highly susceptible to security breaches. Cognitive radio networks exhibit distinct features such as heightened susceptibility to feeble primary user signals, limited availability of shared control channels, and absence of primary user receiver location information. The assailant endeavors to exploit the vulnerabilities of said attributes, as well as others, across multiple strata, protocols, and related technologies [61]. In order to mitigate the risk of malicious node attacks in wireless networks, it is recommended to implement security measures and evaluation policies. Authentication, availability, privacy, reliability, authorisation, and non-repudiation are only few of the security requirements for CR wireless network nodes[62].

2.5.2.1 Authentication in Cognitive Radio Network

It used to protect information from hackers, base stations can use public key cryptography to authenticate themselves to other stations or secondary users/primary users or access points. This might be necessary before an access point or controller allows a particular station to interface with a protected side of the network. Likewise, the client can authenticate the access point in a similar manner [63].

2.5.2.2 Availability in Cognitive Radio Network

The statement implies that authorized secondary users should have consistent and prompt access to information. This entails the appropriate upkeep of hardware and technical infrastructure, as well as the management of systems responsible for storing and presenting information [63].

2.5.2.3 Integrity in Cognitive Radio Network

It involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle from the source SUs nodes to the final destination nodes. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality) [64].

2.5.3 Security Challenges of Cognitive Radio Network

The proposed approach in reference [64, 65, 66] showed the most pressing safety issues with CRNs:

- Power use
- Simplicity Increased Capacity
- Safer spectrum sensing : Secure spectrum sensing is performed to increase spectrum utilization in the network. Each SU performs spectrum sensing and transmits the sensing report to the base station to address the problem of spectrum scarcity. The proposed system is based on secure spectrum sensing challenge to ensure safer sensing scheme for overall connected CR nodes. In addition the proposed system is provide more efficient using of radio resources with secondary and primary base stations.

2.5.4 Still Open Problems

Cognitive radio networks continue to have a high level of security of ongoing concern area, with various unresolved issues that are assessed through the use of security parameters [65, 66].

- Secure Spectrum Sensing.
- Anti-jamming resilience.
- The cross-layered attack in CRNs.
- The multichannel hidden terminal.
- Secure resource sharing in peer-to-peer cognitive radio networks [66].
- The utilization analysis and secure clustering techniques ensuring secure traffic management in cognitive radio networks (CRNs).

2.6 The Secure Cognitive Radio Network System Components

The potential for opportunistic access in cognitive radio networks (CRNs) may be subject to exploitation by malicious secondary users (SUs) who seek to gain access to the spectrum in a self-serving manner. This may be achieved through the manipulation of spectrum sensing information (SSI), which could result in interference to licensed primary users (PUs).The constituents of each network comprise the PU, PU-BS, SU/ SU, SU-BS, and TTP [68].

2.6.1 Advanced Encryption Standard (AES) security Algorithm

The Advanced Encryption Standard, or AES, is a symmetric block cipher. It is implemented in software and hardware to encrypt sensitive data. AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits [69].

Whereas, AES requires the block size to be 128 bits, the original Rijndael cipher works with any block size (and any key size) that is a multiple of 32 as long as it exceeds 128. the key is also arranged in the form of a State of 4 × 4 bytes. As with the input block, the first word from the key fills the first column of the State, and so on. The general steps for implement AES to encrypt the proposed text are :

1- Encrypt the given text and give the byte array.
2- The byte array is converted to corresponding encrypted text.
3- Adding password or encryption key generated by "salt" random generator .
The salt is used as another input of the key derivation function. It is used to prevent brute force attacks using "rainbow tables" where keys are pre-computed for specific passwords. Because of the salt, the attacker cannot use pre-computed values, as he cannot generate one for each salt. The salt should normally be 16 bytes (128 bits) or longer. It also ensures that identical passwords do not have the same derivation results. the AES key will be identical to the generated secret.
4- The result is return as "The encrypted text".

While the general steps for implement AES to decrypt the cipher text are:

1- Checks if a string (Keywords) is founded.

2- Decrypts the given text by the public class for decryption known below require two parameters . the first one represented by (encryption text) or the output (cipher text) and the second for key generator (same salt key)
3- Then convert value of cipher text with specific procedures to convert it and returns into original text.
4- The result returns the decrypt text (plain-text).
5- Figure 2.10 illustrated AES block diagram implemented for the proposed system.

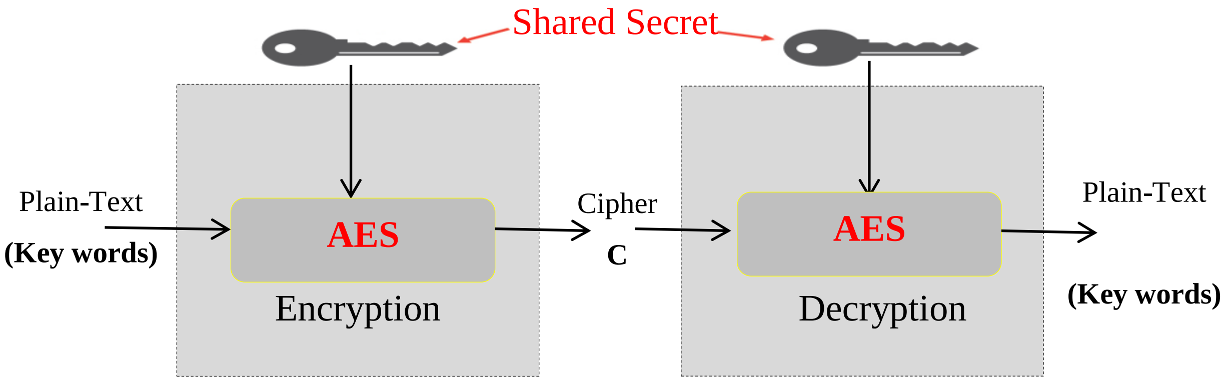


Figure 2.10: AES Block Diagram for the proposed system.

2.6.2 RC5 Security Algorithm

The algorithm is serial as it requires successive exchanges of state entries based on the key sequence. Hence implementations can be very computationally intensive. "RC5 Encryption" Consists of 2 parts:

- Key Scheduling Algorithm (KSA) : to generate, from the key, an initial permutation of the S array (Generate State array)
- Pseudo-Random Generation Algorithm (PRGA): to generate the key stream

Furthermore, XOR keystream with the data to generated encrypted stream. While "RC5 Decryption" process represented by :

- Use the same secret key as during the encryption phase.

- Generate keystream by running the KSA and PRGA.
- XOR keystream with the encrypted text to generate the plain text.

(Plain Text or Keywords **xor** KeyStream) **xor** KeyStream = Plain Text or Data [69].

As noted by this algorithm which left an important impact to ensure authentication in data networks. Particularly, regard to the processing of real time data [69]. Figure 2.11 explained RC5 As used within the proposed system.

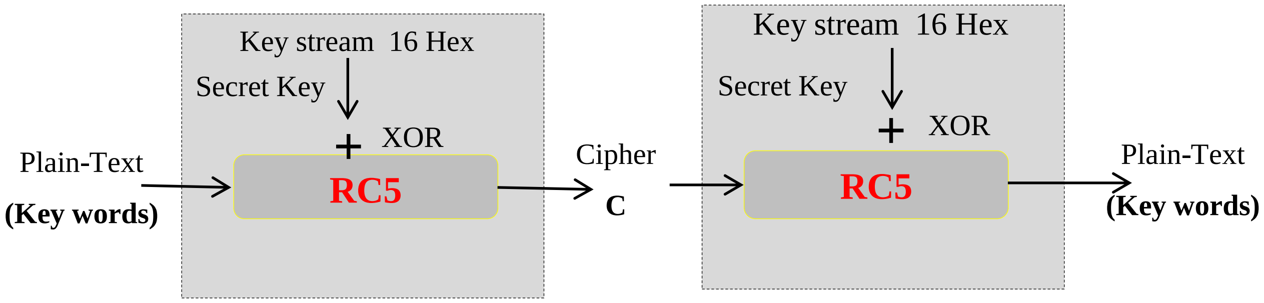


Figure 2.11: RC5 Block Diagram for the proposed system.

2.6.3 Cryptographic Hash Function used in Cognitive Radio Network (Keyed Hash Function, Keyless Hash Function)

A Hashed Message Authentication Code (HMAC), commonly referred to as a keyed hash function, is a cryptographic algorithm that utilizes both a cryptographic hash function and a cryptographic key to generate a message authentication code that is both hashed and keyed. A hash value, sometimes called a message digest, is the fixed-size output of a cryptographic approach in which a hash function and a secret key are used. This technique is obtained employing the "keyed IV" technique, it is possible to establish a set of functions known as keyed hash functions. The function fk, denoted as fk(x) = f(k,x), is a keyed compression function with key length l and input length b. A family of (keyed) functions {Fk}k is associated with any iterated hash construction, such as MD5 or SHA-1. The function Fk(x) is defined for x = x1, x2, ..., xn, such that k0 = k and xn+1 = |x|. Here, ki is obtained by applying the function fki−1 to the input xi, for i = 1, 2, ..., n+1. It is noteworthy that the set of all strings of length l serves as the common space of keys for both the keyed compression functions and the keyed iterated hash functions. This function utilizes a key in conjunction with the message to generate a hash, similar to the HMAC algorithm. There exist two primary methodologies for generating keyed hash codes, commonly referred to as Message Authentication Codes (MACs). The primary and prevalent method involves amalgamating the confidential key and the message information, followed by utilizing a standard cryptographic hashing algorithm to generate a hash value for the amalgamated data. The methodology for merging the key and message is contingent upon the selected algorithm. However, a frequently employed technique is the HMAC standard, which will be expounded upon in the ensuing section [70].

The alternative method does not employ a hashing algorithm in any capacity. The data contained in the message is subjected to encryption through a symmetrical algorithm. Subsequently, the majority of the encrypted data is discarded, leaving only a few bits. This residual data is then utilized as the keyed hash code. It is important to acknowledge that despite the absence of a conventional hashing algorithm, the process of generating a keyed hash code through encryption is still categorized as a keyed hashing algorithm [70].

2.6.4 Elliptic Curve Cryptography (ECC) used in Cognitive Radio Network

Elliptic Curve Cryptography (ECC) is a cryptographic method that employs a key-based approach to secure data encryption. The ECC cryptographic system centers on the utilization of a set of public and private key pairs to facilitate the process of decrypting and encrypting web traffic. The topic of Elliptic Curve Cryptography (ECC) is often deliberated within the framework of the Rivest-Shamir-Adleman (RSA) cryptographic algorithm. RSA cryptography enables unidirectional encryption of various forms of digital information, such as electronic mail, data, and software, through the utilization of prime factorization [71].

Public-key cryptography relies on methods that are easy to compute in one direction but difficult to compute in another. The RSA encryption scheme is based on the computational asymmetry between the ease of multiplying prime numbers to obtain a larger composite number and the difficulty of factoring a large composite number back to its original prime factors [71].

However, to remain secure, RSA needs keys that are 2048 bits or longer. This makes the process slow, and it also means that key size is important. Size is a serious advantage of elliptic curve cryptography, because it translates into more power for smaller, mobile devices. It’s far simpler and requires less energy to factor than it is to solve for an elliptic curve discrete logarithm, so for two keys of the same size, RSA’s factoring encryption is more vulnerable [71].

The utilization of Elliptic Curve Cryptography (ECC) enables the attainment of equivalent security levels with reduced key sizes. In contemporary times, where mobile devices are required to perform increasingly complex cryptographic operations with limited computational resources, Elliptic Curve Cryptography (ECC) presents a viable solution by providing robust security with relatively shorter and faster keys as compared to the widely used RSA algorithm [71].

2.6.5 Digital Signature and Authentication Mechanisms used in Cognitive Radio Network

A digital signature is a kind of electronic signature that uses a mathematical formula to confirm the authenticity and integrity of a communication, such as an email, a transaction made with a credit card, or a digital document. Digital signatures generate a distinct virtual imprint that is exclusive to an individual or organization, and are employed for user identification and safeguarding data in digital communications or records. The digital signature encompasses the email content in electronic mail communication. The utilization of digital signatures is deemed to be more secure in comparison to other types of electronic signatures, as it showed in Figure 2.12 [72].

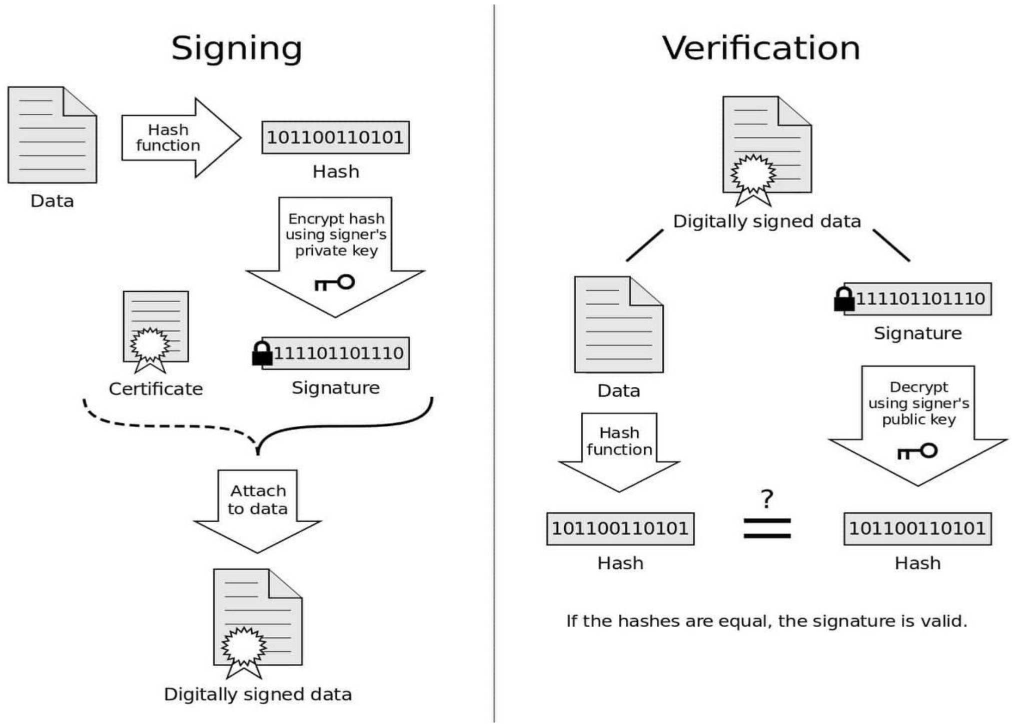


Figure 2.12: Digital Signature and Authentication Mechanisms [72].

2.7 Fuzzy Logic for Primary User Channel Allocation

Spectrum utilization schemes can be more effective in CRNs if they keep their channel selection and handoff decision quick. However, the coexistence of PUs and SUs is characterized as having a highly uncertain deriving factor under different constraints. The parameters and values taken by SUs to detect the presence of the PU or monitor the IT level present a great possibility for impreciseness and incorrectness. Moreover, fading, path loss, and noise add more uncertainty in wireless environment. Furthermore, different decision input variables (e.g., quality of service (QoS) indicators, signal-to-noise ratios, power levels, etc.) are not directly comparable, because they are heterogeneous. Thus, due to the incompleteness of available information to the SU and their qualitative reasoning can make channel selection and handoff decision challenging [73].

The proposed system based on Fuzzy logic model to minimize the SU channel switching rates and to improve the throughput of the system while selecting the best available channel. It is a purely mathematical tool that is used most appropriately for decision making in scenarios where all the input values are imprecise and qualitatively uncertain. Moreover, the information received from the SU is in mostly heterogeneous form, and a fuzzy logic mathematical tool has a quality to transform heterogeneous input into basic homogeneous membership functions. Later, crisp results can be produced using inference fuzzy rules.

The objective of the fuzzy logic scheme is to introduce smarter control systems considering the fact that, most of the time, actual problems can never be professionally stated with the use of mathematical models. However, in order to implement the decision making process, fuzzy logic controllers are used which further need input parameters in terms of fuzzy set. The used Fuzzy Logic model is designed to select the best channel from the list of available channels, which allows the SU to utilize a channel for a long time and eventually minimizes the channel switching rate.

2.8 Attacks in Cognitive Radio Networks

The CRNs TCP/IP model are divided into the five layers are initiated by the spectrum of cyber attacks spans from physical layer attacks to application layer attacks, with the possibility of Cross-Layers attack causing an impact on multiple layers.

1) ***Physical Layer attacks*** : the basic platform layer of TCP/IP model it's the physical medium of the channel that's establish connection among two or more devices with each other for example the network cards, cables, or the atmosphere as wireless networks [74]. These are a group of the most common attacks on physical layer CRNs.

A- Jamming attack : The act of sending a packet during a connection with the intention of exploiting and diminishing the signal is commonly known as a denial of service attack[74].

B- Primary Users' Location attack : The attack type that involves direct targeting of devices after identifying the primary user's location is widely regarded as one of the most perilous [75].

2) ***Data Link Layer attacks*** : The concealment of the physical medium's underlying hardware details is a characteristic of this layer, whereby attackers may exploit vulnerabilities in MAC address strategies [76].

A- Spectrum Sensing Data Falsification (Byzantine attack) : Malicious node will send a falsified spectrum Sensing information for misleading and manipulate the decision-making process, prevent secondary users from using the existing spectrum hole, bring the spectrum band to access into the channels and cause excessive interference or reduce throughput to legitimate users in CRNs [77].

B- ***Control Channel Saturation DoS Attack (CCSD)*** : due to the distribution communication, the process is necessary to connect nodes with each other and multiple overlapping manner in a multi-hop CRN, within MAC-layer control frames are exchanged to preserve the channel [78].

3) ***Network Layer Attacks***: Similar to conventional wireless communication networks, CRNs may take on a variety of network topologies, including those with and without an underlying physical infrastructure (ad hoc and mesh) and those that combine the two (hybrid networks, such Wireless Sensor Networks) [79].

4) ***Transport Layer Attacks*** : The perpetrator within Cognitive Radio Networks (CRNs) endeavors to capitalize on susceptibilities during the transmission session, specifically during the establishment of connection processes between nodes [80].

5) ***Application Layer Attacks*** : It is possible that an assault on the lower strata could yield unfavorable consequences for the application stratum within CRNs [81] .

Table 2.1 presents a summary of layered attacks and cross-layer attacks that are commonly launched against cognitive radio networks (CRNs) [82].

Table 2.1: Cross-layer attacks and their defenses.

Attack	**Targeted layer**	**Common Countermeasure**
PUE Attack	Physical Layer	Cryptographic Authentication
OFA Attack		Prior identification the threshold value [52],

		Intrusion Detection System (IDS)
Jamming Attack		Determine and keep track the location identification of the primary user's, Frequency hopping spread spectrum Technique
Eavesdropping Attack		Encryption Techniques
Primary Users' Location Attack		changing the density of signals irregularly
LA Attack		Control Environment especially during learning phase, Constant Reevaluation [56].
Byzantine Attack	Data Link Layer	Misbehavior Detection System (MDS) [64], Cooperative neighboring cognitive radio nodes (COOPON) (Minho et al, 2013), trust and reputation metrics
CCSD Attack		Trust as Detection Mechanism
SCN Attack		Trust as Detection Mechanism
Hello Attack	Network Layer	Symmetric Key based algorithm
Sinkhole Attack		Geographic routing protocols [55]
Sybil Attack		identity validation
Ripple effect Attack		checked and validated necessary information
Key Depletion Attack	Transport Layer	Security Protocols [83]

2.9 Evaluation Metrics

The proposed system is evaluated with different evaluation metrics sorted as follows :

2.9.1 Throughput

Throughput is described as the ratio of the number of packets sent and received to the total required time. and the used equation as [84] :

$$\boldsymbol{Throughput} = \frac{\boldsymbol{Total\ Number\ of\ sent\ and\ received\ packets}}{\boldsymbol{Time}} \qquad (2.1)$$

2.9.2 Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is the ratio of total number of data packets received at the destination to the total number of data packets transmitted by the source. It is calculated as [84]:

$$\boldsymbol{PDR} = \frac{\text{Number of packets received at destination}}{\text{Total number of packets sent}} \qquad (2.2)$$

2.9.3 Packet Loss Ratio

It represents the ratio of the number of lost packets to the total number of sent packets[84].

2.9.4 Probability of Channel Collision

The probability of collision during random channel access for number of SUs contending for number of sensed idle PUs channel. The probability of collision increases as the number of SUs increases for a fixed number of idle channels. This in turn decreases the average number of successful SUs. The number of idle channels available to SUs in a CRN depends on the primary user traffic intensity. At high primary load, there are very few idle channels, hence the probability of collision increases [85].

For example how to calculate probability of collision, It define t as the time required for PU to become active from starting point of data transmission slot in the current frame. The collision duration of the current frame with PU can be expressed as it calculated in equation (2.3) [85] :

$$\textbf{\textit{Probability of Channel Collision (t)}}= \begin{cases} T-t, 0\le t\le (T-t) \\ 0, \quad t\ge (T-t) \end{cases} \quad (2.3)$$

2.10 Cognitive Radio Networks Security Simulation Tools

2.10.1 OMNET++

The simulator is an open-source software that utilizes a graphical user interface to present internal events in a user-friendly manner to the end-user. The Omnet++ framework offers a modular library and streamlined debugging/tracing capabilities that do not require additional coding efforts from the programmer. The application of a novel cognitive model to an established wireless sensor network (WSN) is facilitated within the cognitive radio network through the incorporation of the Castalia framework simulator. This enables the simulation of diverse CWSN devices featuring distinct radio standard interfaces [86].

2.11 Cognitive Radio Network Security Challenges

The execution of the suggested study within the initial network structure and configuration has encountered various challenges can be succinctly sorted as follows:

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.

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.

Free Secure library: Among the most challenging aspects of network design is the implementation of a robust security system. The absence of security libraries has facilitated their effortless loading and development. This outcome has been attributed to the varying releases of simulator tools and library integration with contemporary versions, as well as the concurrent implementation of encryption algorithms and security protocols. The consumption of time is deemed significant, particularly for researchers who are constrained by time. Conversely, the "OMNET++" platform features the crypto++ library, which incorporates certain security models. However, as previously elucidated, further refinement and enhancement is required.

Learning Time : due to the importance of this simulator for academic sides to implement different communication mechanism and simulate different research trends. It's should have more attention in the organization before arrive to master or PhD degree . The proposed system implementation encountered the lack of prior experience to implement the proposed work .Where researcher must take into consideration amount of time to learn and apply models. as well as, how to handle tools and extensions libraries.

Chapter Three

The Proposed Approach

3.1 Introduction

Cognitive Radio is widely regarded as a contemporary methodology for enhancing the efficacy of spectrum utilization in wireless environments. The system is constructed by using a software-defined radio and is characterized as an intelligent wireless communication system that possesses environmental awareness. It employs a methodology of comprehension and assimilation from the surrounding environment. Furthermore, it adapts to changing in the input parameters stimuli which are affected on decision making process.

The proposed system improved the security of cognitive radio networks in environmental applications by incorporating a content-aware feature that facilitates the management of transmission messages, such as TCP ping, FTP file statistics, and UDP for big image uploading, using two secure methods: the first method is the Encryption Standard method with (AES, RC5 encryption algorithms as the data message in OMNET++ , and channel allocation with fuzzy logic method, the second method is cognitive trusted party (CTP) approach to provide integrity with SHA-3 and authentication with ECC. It has been advanced for an astute security mechanism within a CRN that functions in accordance with the nature of the input packet received by the system. Stated differently, the process relies on the filtration of file uploads that are shared among the cognitive radio (CR) nodes within the network. Furthermore, the analysis is predicated on these specific data categories.

Moreover simulation results from both system case studies : the first security system with AES and RC5; the second security system with SHA-3 for integirty and ECC for authentication purpose all these modules as well as, each algorithm are implemented to simulate real work for each concern and to give the same behavior for the actual module.

3.2 The Proposed Security System for Cognitive Radio Networks

The proposed secure system is consists of two main frameworks as follow :

3.2.1 Security system with Crypto system AES, RC5 Encryption Algorithms

In the first stage of simulation run time, it initialized input encrypted packets (Data) exchanges among cognitive radio nodes, and their equivalent encryption CipherText generated from the c# programming language as AES, and RC5 cipher Text. Through, secure system based on AES, RC5 cryptography, and Fuzzy logic channel throughput enhancement. The security approach effected on the throughput due to the delay is increased, so to make enhancement in state of throughput and data bandwidth in the proposed system, the fuzzy logic channel allocation applied as the fuzzy interference system which brings down the switching rate of the secondary users to enhance the overall performance.

All these processes will be entered to CRNs Architecture Layers (DATA & CTRL Links). Subsequently, proposed CRNs implementation in environment application will be build results and statistics. In Figure 3.1 initialized the proposed system with encrypted cipher text. All of these names are categorized as a sample parameters to simulate the proposed environment. So, the block of letters which are supports the proposed encryption algorithm entire the security system. 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 with same Hexadecimal-value in (AES, RC5). Each of these encryption algorithm has encrypted length as plaintext length equal to (88 characters of AES, 30 characters of RC5) which are classified and selected from saved string pool to exchange among cognitive radio environment.

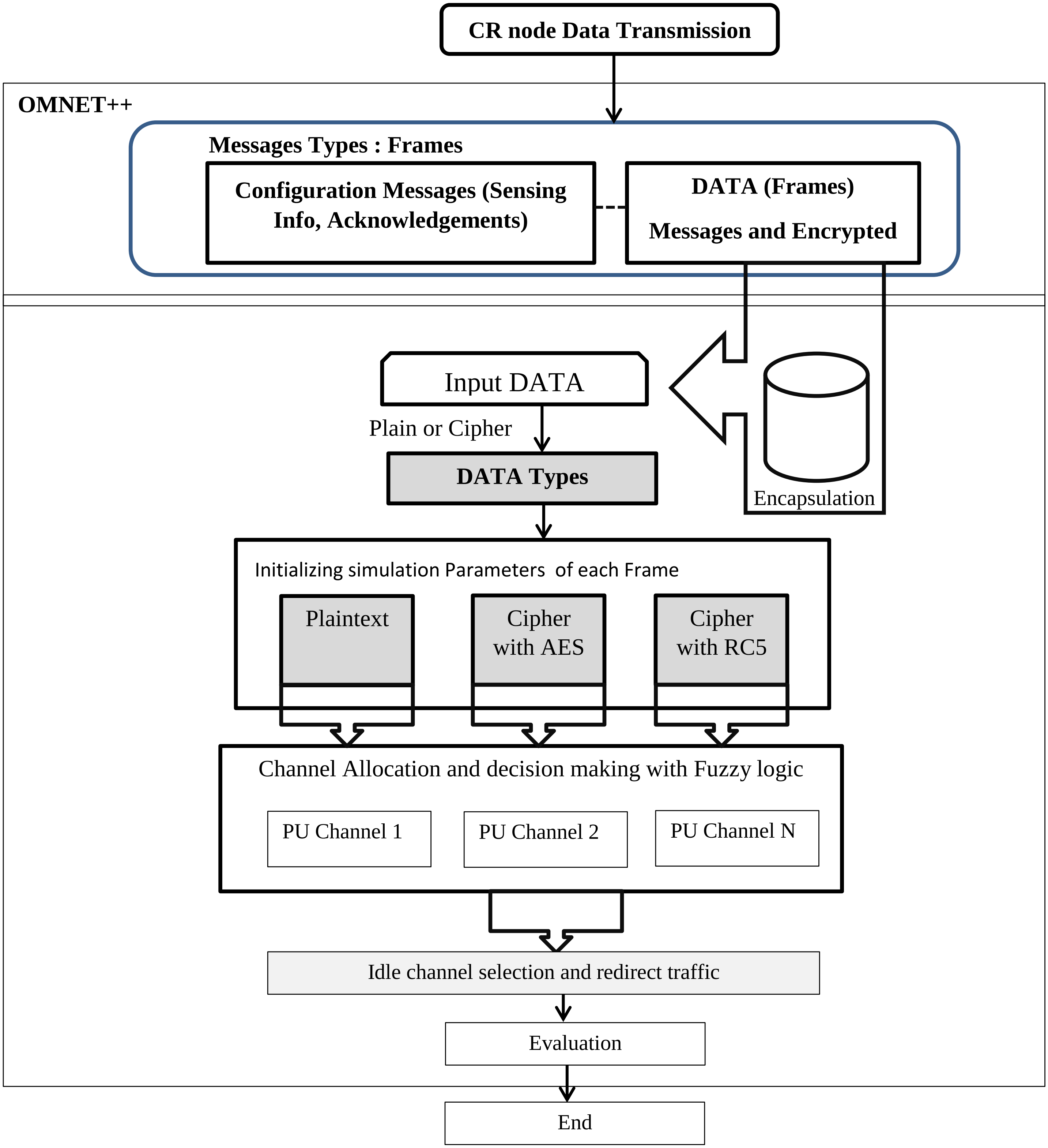

CR node Data Transmission
OMNET++
Messages Types : Frames
Configuration Messages (Sensing Info, Acknowledgements)
DATA (Frames)
Messages and Encrypted
Input DATA
Plain or Cipher
DATA Types
Encapsulation
Initializing simulation Parameters of each Frame
Plaintext
Cipher with AES
Cipher with RC5
Channel Allocation and decision making with Fuzzy logic
PU Channel 1
PU Channel 2
PU Channel N
Idle channel selection and redirect traffic
Evaluation
End

Figure 3.1 : Fuzzy logic Block Diagram of the CRN Security Scheme.

Figures (3.2) and (3.3) demonstrate the utilization of fuzzy logic resource channel allocation by the primary and secondary users, two key elements of cognitive radio networks. This approach enables opportunistic access to frequency bands by cognitive users without causing interference to licensed users when the acknowledge channels are occupied and unavailable for use. It is advisable for cognitive radio users to steer clear of collision states during the transmission process. The radio spectrum of the first user's idle state may be obtained by the secondary user, as busy states are indicative of working periods or presence of primary users.

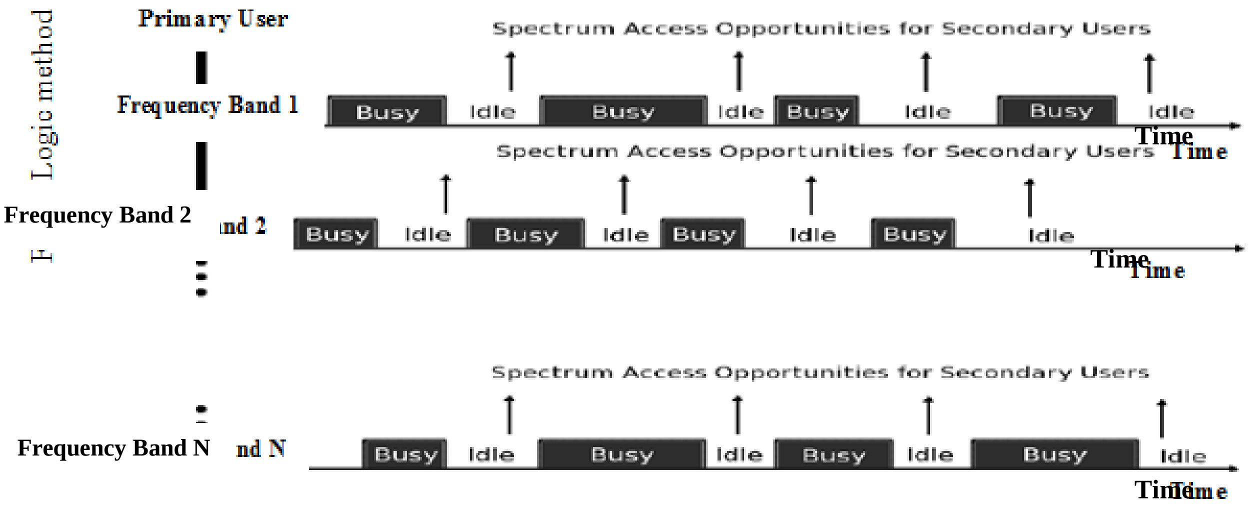


Figure 3.2: Fuzzy logic busy/idle state for main user spectrum access.

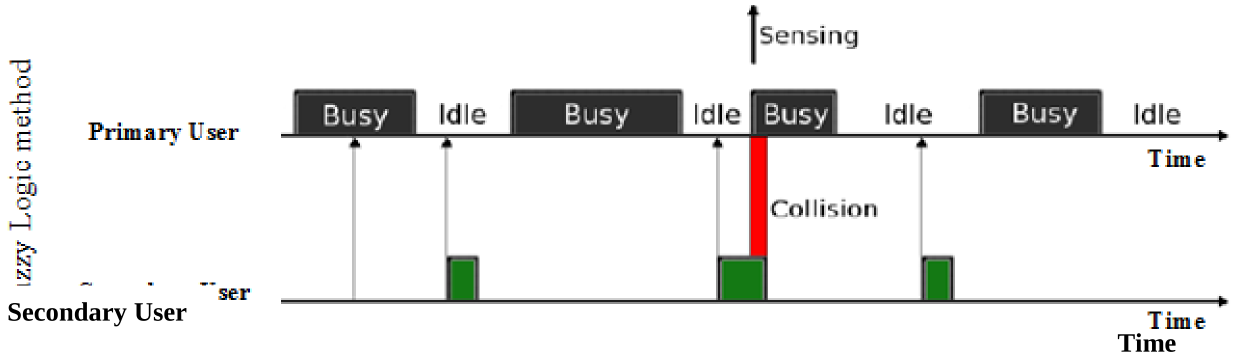


Figure 3.3: behavior of Primary and secondary users with Fuzzy logic.

3.4.1.1 The used DATA packets

The initial segment of the packet involves spectrum sensing in CR for the purpose of identifying an available channel for transmitting data messages, while also ensuring that no harm is caused. The primary user, commonly referred to as the GSM, determines the availability of a channel by assessing whether it is free or occupied.

Upon initiation of the simulator, encrypted data is provided as keyword parameters, which serve as the initial input state for the cognitive radio network environment. Each data type possesses a distinct format for encapsulating its data. The header bits of the frame serve to establish its fundamental characteristics, while the payload segment, which can range in size from 0 to 254 bytes, is responsible for conveying the primary data.

Proposed channel : This is related to the identification of the available channel that is utilized as an idle medium for transmitting messages. This is determined by Fuzzy logic approach for channel allocation as primary channel spectrum bands. It provide list of active frequency bands provided by primary users in specific time when primary user not present.

Frame ID : The item has been configured to function as a slot location. The identification of the slot for frame transmission is denoted by the frame ID. In a given communication cycle, a frame ID is utilized only once on a single channel. Every frame is associated with a distinct frame ID that corresponds to a unique slot. The frame identifier spans a numerical range of 1 to 2047, represented in binary as 00000000001 to 11111111111, with the exception of frame ID 0 which is deemed invalid.

Data length : The purpose of this is to denote the dimensions of the encapsulation field. The encapsulation field size is determined by encoding it with the quotient of the number of encapsulation data bytes divided by two, which is equivalent to multiplying the data length by two).

Source (Src) : It specifies the MAC address of the source nodes.

Destination (Des) : it explained MAC address of destination nodes

Control (Ctrl) : It specifies control information such as RTS/CTS on the mac layer to minimize message collisions.

Association : It provides the security mechanism that is used to encrypt data in cognitive radio wireless networks, which is represented by the AES. It also specifies the RC5 encryption method.

Encapsulation : It includes security elements for the proposed system (plain text and CipherText) that are based on "AES, and RC5 algorithms." These algorithms are built from an external library by using the programming language c#, and then pass cipher text into secondary user data fields to exchange with other SUs.

Data (Cipher-text) : the input keyword that is entered during the first simulation state for the application being utilized is specified by this field.

Figure 3.4 showed the used Data link layer frame with the used fields. The security fields are explained as the encapsulation and association for the used class of algorithms and cipher text is sorted in data field.

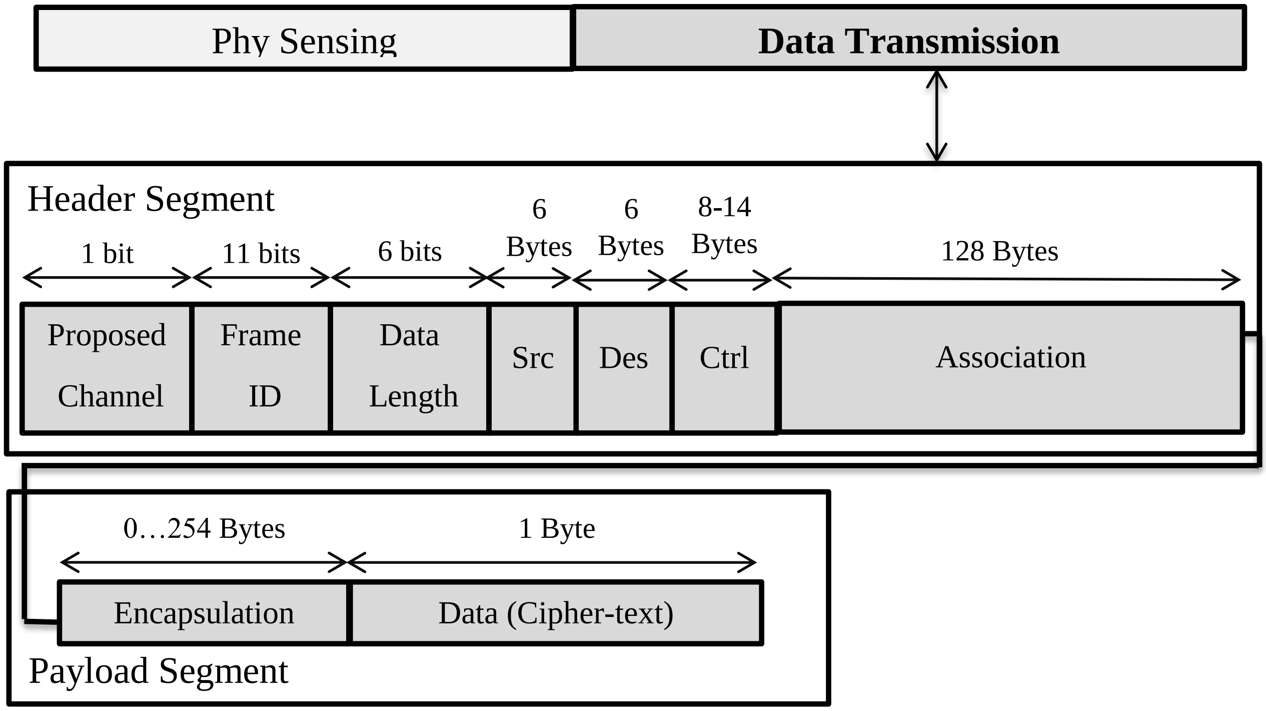


Figure 3.4: the proposed DATA packet Format.

3.4.1.2 The used Control (Sensing Info) Packets

The sensing information packets is managed by Fuzzy logic channel allocation method which is used as RTS & CTS packets used to enhance the virtual carrier sense process. RTS/CTS is simulated to prevent collisions occurrence. RTS (Request to Send) Frame is 14 Bytes in length. Each octet represented by (8 bits). The RTS (Request to Send) frame comprises three distinct fields:

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, the receiver address pertains to the MAC address of the designated station to receive the frame.
3. TA (Transmitter Address) : 6 octets or 6 Bytes, the Transmitter Address denotes the Media Access Control (MAC) address of the station responsible for transmitting the frame.

Octets: 2	6	6
Duration	RA	TA

MAC Header : Control Field

Figure 3.5: the proposed RTS Frame Format

Besides, the CTS (Clear to Send) and Acknowledgement(ACK) packets are showed as RTS and ACK frames . It is 8 bytes in length for each frame.

1- Duration : 2 octets = 16 bits .
2- RA (Receiver Address) : 6 octets = 48 bits.

Octets: 2	6
Duration	RA

MAC Header : Control Field

Figure 3.6: the proposed CTS Frame Format

Acknowledgement packets are sent to transmitter to confirm the data packet received by receiver node. Duration is always set to 0. It is worth noting that the field (Duration) is just within (ACK) frame. It is always set to zero in order to represent the next frame request.

Octets: 2	6
Duration	RA

Figure 3.7: the proposed Acknowledgement Frame Format

3.4.2 Security approach with Cognitive Trusted Party (CTP)Model

The second instance of the proposed security system is founded upon an innovative framework and arrangement. The network topology is SUs, BS-SUs, CTP, Primary Users, BS-PUs, and network elements(Access Point, Router). The proposed cognitive network support wireless communication and mobility with different mobility types as linear and random mobility with dynamic spectrum access for data type, node characteristics, and channel characteristics.

Data type used for environmental application as Text, Image, Files.

- Text data type: It is represented as temperature reads, earthquake, and wind ratio. The text reading size is (2 B to 20 B).
- Image data type: It is represented as images of earthquakes or changes in desert areas. In some cases, they are pictures from camera sensors, and they record pictures and snapshots of rain and wind of different sizes. The image size is (10 KB to 30 KB)
- File data type : It is represented as statistics file with excel file uploaded and shared among nodes in the network. The file size is (100 KB to 800 KB).

In addition, the network topology description is as follow :

- Secondary Users (SUs) : It is wireless cognitive radio nodes used to send and receive environmental packets.
- Base station-Secondary Users (BS-SUs): It is used in the proposed system to manage spectrum radio sensing, suggest optimal PU channel (channel allocation), decrease computation process (enhance network performance) on secondary users, and to secure authentication for nodes in cognitive radio networks as it provide key exchange and it establishes secure session between SU nodes, and CTP manager.

  CTP provide session key to each BS-SUs. Each SU node contains public key as session key which is provided by base station. Authentication is provided with session key (public key: ECC method) to make a connection to the network by authorized elements.
- Cognitive Trusted Party(CTP) : It is the network manager which is responsible for network overall for security purposes. It also passes channel

allocation from primary base station to the SUBS. The security part in this elements is authentication and integrity. Authentication is with ECC method between two cluster (BS-SU, and BS-PU). Besides, integrity with SHA-3 is applied to ensure environment data is not modified during the round trip of transmission from the source secondary node to the destination secondary node. SHA-3 is programmed as messages digest (binary serial) added to the encapsulated field and it is matched when it arriving at the destination as it corrected not modified.

- Primary Users : It is presented as primary user node (licensed node) which provides channel frequency bands to the secondary users to increase bandwidth of the radio spectrum of cognitive radio network.
- Base station-Primary Users (BS-PUs) : It is presented as the management point for primary users to collect and redirect authenticity features with CTP and channel state among primary user elements. When channel state is free or idle it redirect the number of primary user and channel frequency band and time duration to be idle or busy.
- Network Elements(Access Point, Router) : They are used as gateway and bridge devices to provide connectivity and network administration. Access point provides coverage area for wireless communication range. Router provided redirection packets to connect network elements. Figure 3.8 shows network elements in the proposed system.

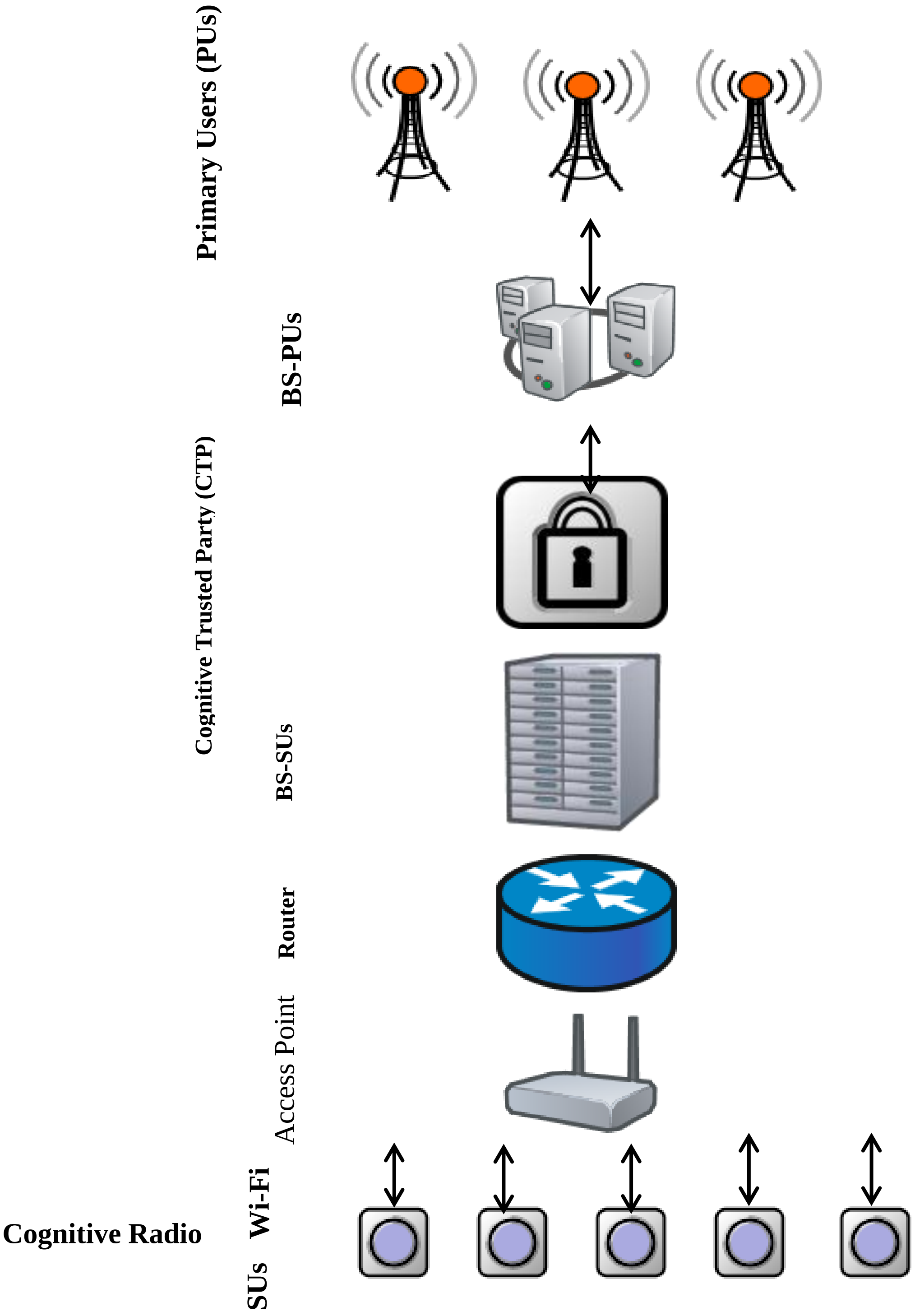


Figure 3.8: The proposed cognitive radio Network topology components.

Figure 3.9 shows authentication process in the proposed secure cognitive radio system.

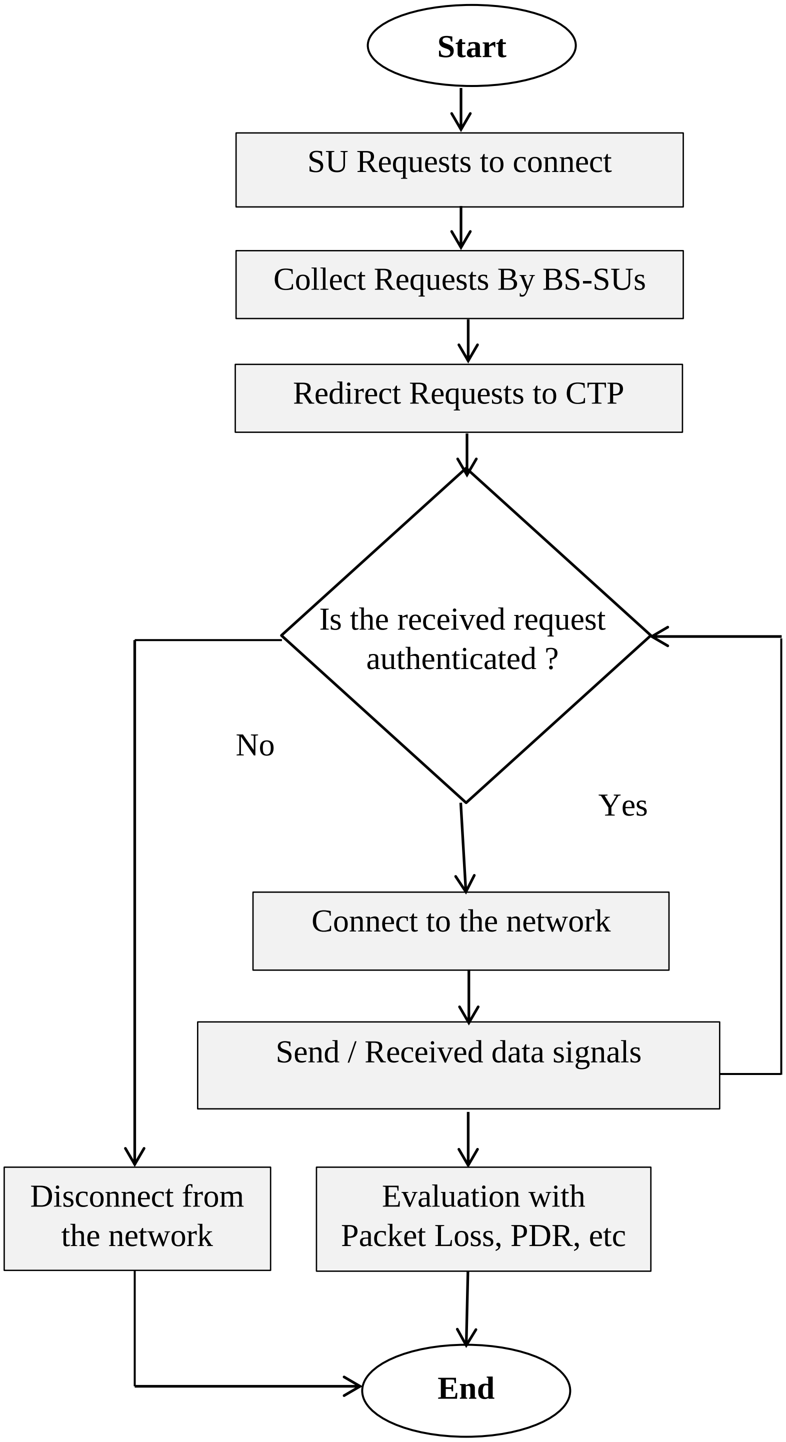

Start
SU Requests to connect
Collect Requests By BS-SUs
Redirect Requests to CTP
Is the received request authenticated ?
No
Yes
Connect to the network
Send / Received data signals
Disconnect from the network
Evaluation with Packet Loss, PDR, etc
End

Figure 3.9 : The authentication process in the proposed system.

In the proposed network, it can be observed from Figure 3.10 that the CTP employs an ECC public key cryptosystem for the purpose of generating asymmetric key pairs, namely the sender Pr-CTP and the sender Pu-CTP. The proposed model involves the transmission of keypairs by the TTP to the BS-PU, BS-SUs, and SUs, along with the TTP's ID. Subsequently, each node decrypts this message using the public key of the CTP.

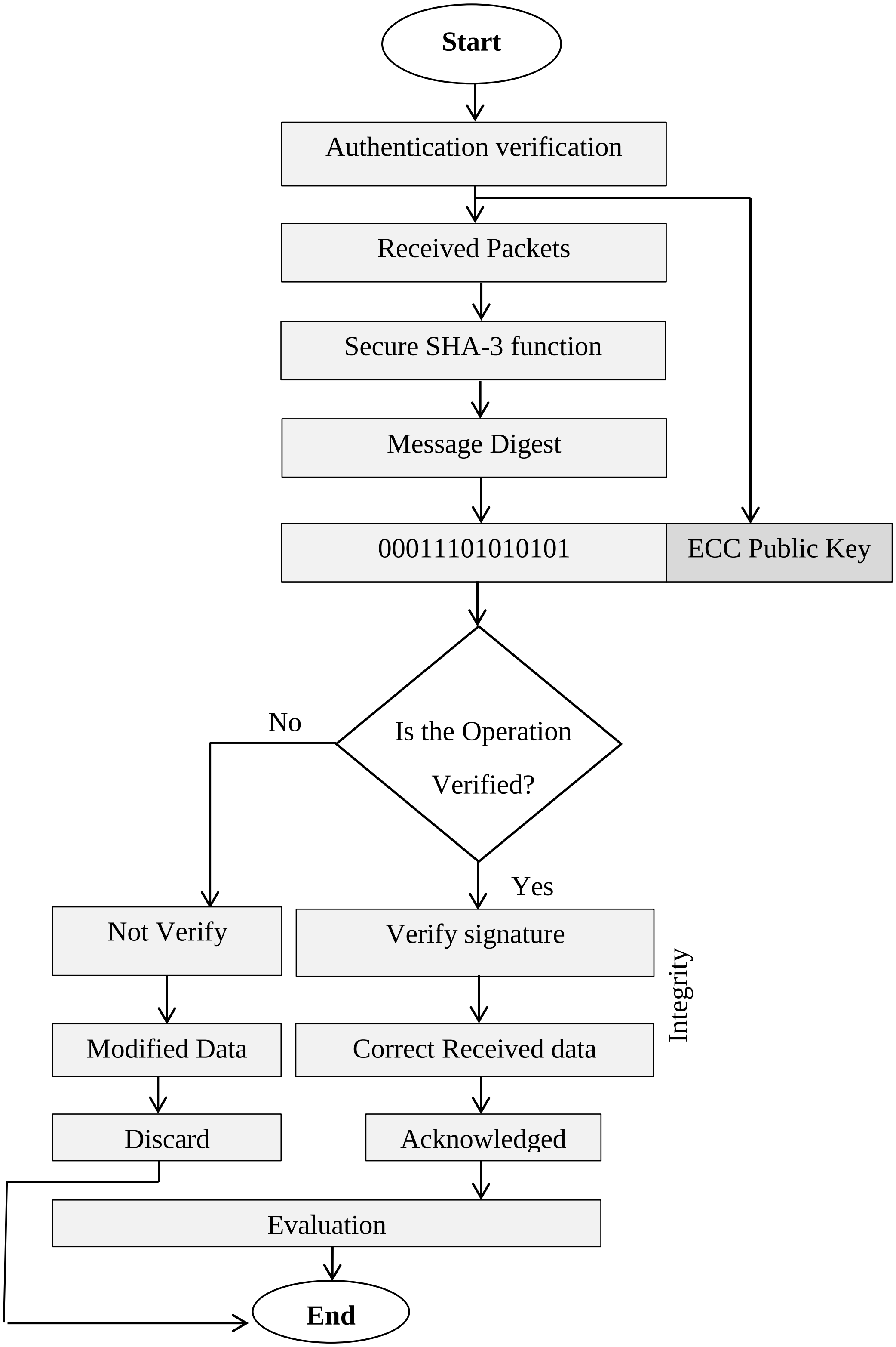


Figure 3.10:The proposed Authentication and integrity in the proposed system.

The SHA-3 function then appended to the original message to produce a digitally signed message that sent over the network. The output is subsequently appended to the initial message, thereby creating a digitally signed message that is then transmitted across the network. The receiver verify the digitally signed message using the sender public key (Pu) to decrypt the encrypted hash value and then apply the proposed hash function to the original message, the receiver then compare the two hash values, the digital signature is valid and message verified and accepted if the two hash values are equal, it showed in Figure 3.10

Chapter Four

The Implementation and Results

4.1 Overview

This chapter explain the implementation system and the generated results of the proposed system with the two main secure systems as follow:

The first secure system of cognitive radio with the 1st case study showed the AES encryption algorithm. The 2nd case study is the RC5 encryption algorithm. The 3rd case study is the normal state of cognitive radio network without security system. The data signals are generated with the AES, RC5 encryption algorithms as the data message in OMNET++. Besides, the proposed system has been implemented and tested with authentication (ECC), and Integrity (SHA-3) to provide secure data transmission and secure channel allocation of secondary users without interference with primary users.

The second secure system consists of four cases : The 1st is the state of without secure approach and interference. The 2nd is the authentication case with ECC cryptosystem to provide authenticated nodes (SUs, and PUs) to connect and transmit data without allowing to the unauthorized node to communicate and get channel allocation. The 3rd case study is to provide data integrity to each data type transmitted from the source nodes (SUs) to another secondary node. The 4th case is the integrated approach between authentication and integrity is to provide better secure system for each network element connected to the cognitive radio network.

Table 4.1 shows the cipher text generated with each algorithm; in addition to, encryption time, decrypt, time and the fuzzy logic method for max and min cipher text with “AND” logic operation.

Table 4.1 : system comparisons of AES compared with RC5 algorithms.

	AES			**RC5**		
Plain-Text	101110010101110	1011100101011101011100101	010111011111010110111001010110	101110010101110	1011100101011101011100101	0101110111111010110111001010110
Cipher-Text	VvjtbgGV9Jm2u7rmsCe65wKzPTw5jtS38n2tVEGi2yFNYwbKZnGj8Ac3frdQlmAg	bADbmBRpEXiJCwb9R+JlmZA9VMv+gzdujb+CfqhnCgZhnaBZWs8oAshLs3Mfskyi	WwJmv2xxbjsDrW0yAP9hTDpqeWLpEobQ4BcdSIRa+ngfSfGV9Jm2u7rmsCe65wKzPTw5jtS38n2tVEGikpYlBw==	œGY§) حزه□ع±ة(	œGY§) حزه□ع±ة(U ©p±Q‹du	FY§(جز□غ±ةه (U¨p°Qٹet"، 06ƒ
Input size in bits	15 bits	25 bits	30 bits	15 bits	25 bits	30 bits
No. of cipher characters	64	64	88	15	25	30
Encrypt. Time	519 ms	856 ms	874 ms	232 ms	256 ms	289 ms
Decrypt. Time	345 ms	748ms	765 ms	215 ms	260 ms	271 ms
Output size in Kbytes	0.512 Kb	0.704 Kb	0.704 Kb	0.12 Kb	0.2 Kb	0.24 Kb
Fuzzy logic strength	0.512 * 0.704 = 0.3604			0.12 * 0.24 = 0.0288		
RANDOM KEY of AES	c89dfdb0-ae50-4b5c-a107-4994feb284ce					
RANDOM	ab48495fdjk4950dj39405fk					

KEY of RC5	

4.2 The 1st security system for cognitive radio network

It is applied on the simulated cognitive radio network with two main elements : secondary user, and primary user. The security system is programmed with visual studio and injected in OMNET++.

4.2.1 The AES security algorithm in CRNs

It is based on the implementation of AES in C# to generate data signals passed to the OMNET++ as the data signal; it is used as 88 Byte of block encrypted message. It is implemented with three cases : (4 SUs, and10 PUs ; 8 SUs and 20 PUs; 16 SUs and 30 PUs).

4.2.1.1 The case of 4 SUs and 10 PUs in AES security system

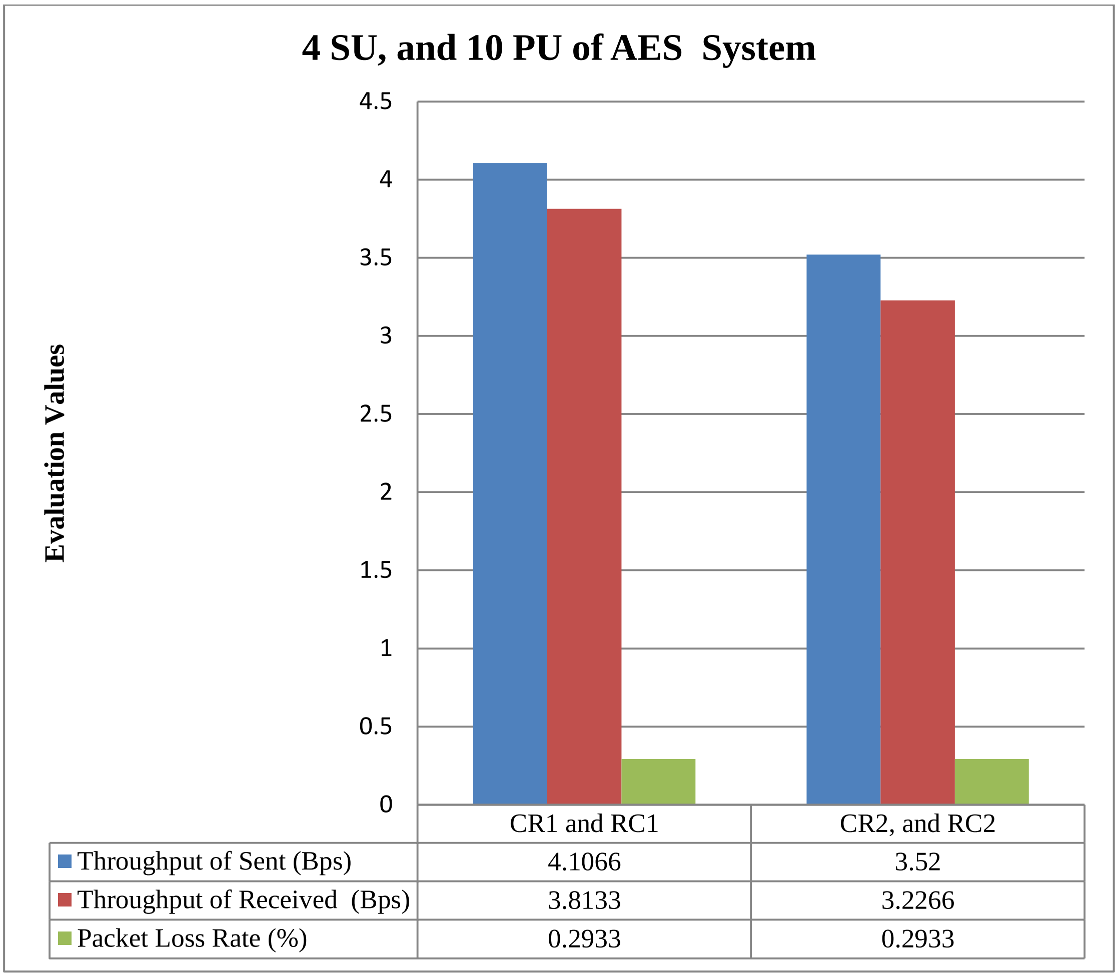
The initial instance of the system comprises 10 primary users and 4 secondary users. Table 4.2 displays the specifics of the data traffic. The network is used with 2 secondary users as transmitters and 2 secondary user as receivers. Each network elements secondary users send data signal of size 88 bytes from sender to the receiver node; besides packet loss rate is calculated from the distinction between packets that have been sent and those that have been received while the PDR is calculated from the division received to the sent packets.

Table 4.2: Throughput of encapsulated/decapsulated, and Packet Loss Rate of 4SUs, and 10 PUs in AES case study.

Network Element		**Payload Throughput / Bps (Encapsulated/Decapsulated)**		**Packet Loss Rate (%)**	**PDR %**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	4.1066	3.8133	0.2933	92.8578%
CR 2	RC2	3.52	3.2266	0.2933	91.6648%

Data signal size	88 Byte

Figure 4.1 showed the evaluation throughput of sent throughput of received, and packet loss rate in case of AES encryption algorithm. It showed that the increased number of idle channel effects increased throughput due to the bandwidth is increased so lost packet and overloading under control.



	CR1 and RC1	CR2, and RC2
🟦 Throughput of Sent (Bps)	4.1066	3.52
🟥 Throughput of Received (Bps)	3.8133	3.2266
🟩 Packet Loss Rate (%)	0.2933	0.2933

Figure 4.1 : AES case study transmitted and received throughput and loss of packets rate of 4SUs and 10PUs.

Table 4.3 presents the aggregate count of transmitted and received packets, along with the corresponding rate of packet loss.

Table 4.3: Number of sent/received packets, loss packets of 4SUs, and 10 PUs in AES case study.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	14	13	1
CR 2	RC2	12	11	1

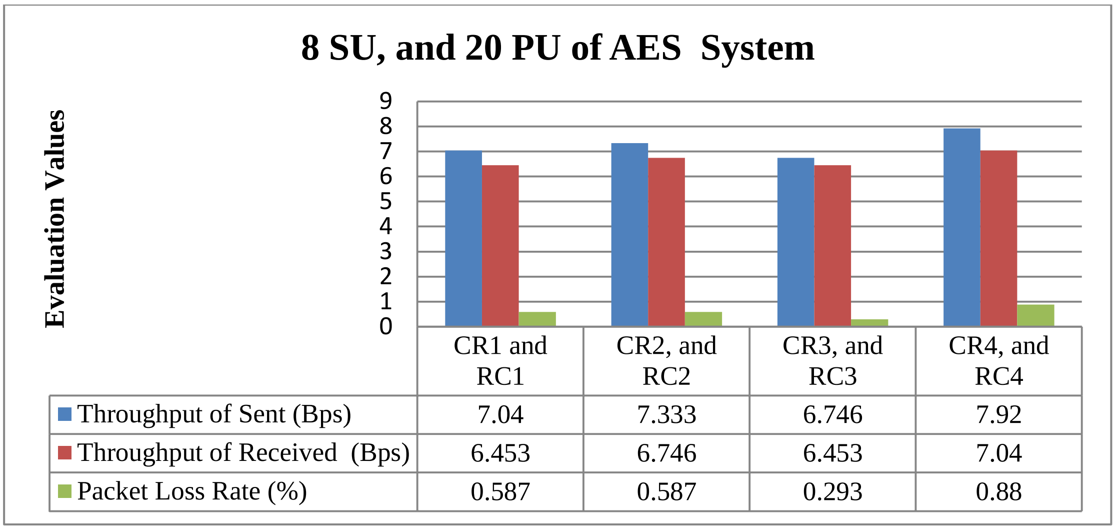
4.2.1.2 The case of 8 SUs and 20 PUs in AES security system

It shows the better case of throughput due to the increasing number of idle channels used by secondary users to transmit data signals from node to node. Table 4.4, and Figure 4.2 show the throughput and packet loss rate in case of 8 SUs, and 20 PUs in AES case study. AES system increase size of ciphertext or data signal that will be exchanged among secondary users which takes time for packets to travel from the source node identified to the node of the destination that is impacted.

Table 4.4: Throughput of encapsulated/decapsulated, and Packet Loss Rate of 8 SUs, and 20 PUs in AES case study.

Network Elements		**Payload Throughput / Bps (Encapsulated/Decapsulated)**		**Packet Loss Rate (%)**	**PDR %**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	7.04	6.453	0.587	91.6619%
CR 2	RC2	7.333	6.746	0.587	91.9951%
CR 3	RC3	6.746	6.453	0.293	95.6567%
CR 4	RC4	7.92	7.04	0.88	88.8889%
Data signal size		88 Byte			

AES case study transmitted and received throughput and loss of packets rate of 8 SUs and 20 PUs. It showed the enhancement in throughput due to increased number of primary user compared with secondary user. The total sum of throughput sent packets is 29.039 Bps, the total sum of throughput received packets is 26.692 Bps and the lost packets is 2.347 %.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	7.04	7.333	6.746	7.92
🟥 Throughput of Received (Bps)	6.453	6.746	6.453	7.04
🟩 Packet Loss Rate (%)	0.587	0.587	0.293	0.88

Figure 4.2 : AES case study transmitted and received throughput and loss of packets rate of 8 SUs and 20 PUs.

Table 4.5 showed the number of sent/received packets, loss packets of 8 SUs, and 20 PUs in AES which represented packets encapsulated with AES.

Table 4.5: Number of sent/received packets, loss packets of 8 SUs, and 20 PUs in AES case study.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	24	22	2
CR 2	RC2	25	23	2
CR 3	RC3	23	22	1

CR 4	RC4	27	24	3

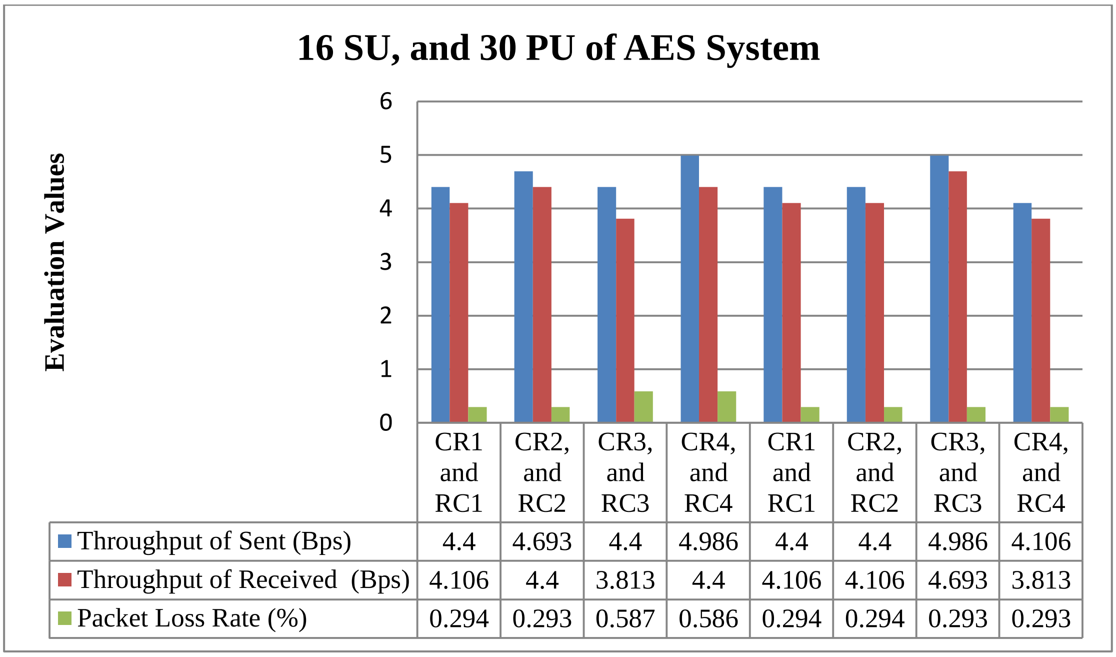
4.2.1.3 The case of 16 SUs, and 30 PUs in AES security system

It is based on the AES encryption data signals in each 16 cognitive radio nodes to exchange signals among them, as it shows the evaluation metrics in Table 4.6. When number of nodes increases the loss rate increases due to the increasing no-acknowledgement packets to be discarded from the destination node due to the waiting time or overload in the large network. Packet loss rate is calculated by packets sent - packets received as the measurement of network performance when this value is decreased the network performance is increased.

Table 4.6: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 16 SUs, and 30 PUs in AES case study.

Network Elements		**Payload Throughput / Bps (Encapsulated/Decapsulated)**		**Packet Loss Rate (%)**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	4.4	4.106	0.294
CR 2	RC2	4.693	4.4	0.293
CR 3	RC3	4.4	3.813	0.587
CR 4	RC4	4.986	4.4	0.586
CR 5	RC5	4.4	4.106	0.294
CR 6	RC6	4.4	4.106	0.294
CR 7	RC7	4.986	4.693	0.293
CR 8	RC8	4.106	3.813	0.293
Data signal size		88 Byte		

It showed the AES case study transmitted and received throughput and loss of packets rate of 16 SUs and 30 PUs. The total sum of throughput sent packets is 36.371 Bps, the total sum of throughput received packets is 33.437 Bps and the lost packets is 2.934 %.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	4.4	4.693	4.4	4.986	4.4	4.4	4.986	4.106
🟥 Throughput of Received (Bps)	4.106	4.4	3.813	4.4	4.106	4.106	4.693	3.813
🟩 Packet Loss Rate (%)	0.294	0.293	0.587	0.586	0.294	0.294	0.293	0.293

Figure 4.3: AES case study transmitted and received throughput and loss of packets rate of 16 SUs and 30 PUs.

Furthermore, Table 4.7 presents the quantity of transmitted and received packets for a security system by utilizing the AES encryption algorithm.

Table 4.7: Number of sent/received packets, loss packets of 16 SUs, and 30 PUs in AES case study.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	15	14	1
CR 2	RC2	16	15	1
CR 3	RC3	15	13	2

CR 4	RC4	17	15	1
CR 5	RC5	15	14	1
CR 6	RC6	15	14	1
CR 7	RC7	17	16	1
CR 8	RC8	14	13	1

4.2.1.4 The case of 16 SUs, and 30 PUs in AES security system with Fuzzy Logic Approach

The case of fuzzy logic is implemented to enhance network performance in case of the less throughput as the 16 SUs and 30 PUs. The utilization of a fuzzy logic methodology facilitates adaptability in switching and restricts the switching action to instances at which the point level of interference exhibits by the secondary client exceeds the predetermined threshold level. The implementation of this methodology serves to alleviate the necessity for frequent transitions between secondary users, thus enhancing the efficacy of the CRN with respect to its throughput.

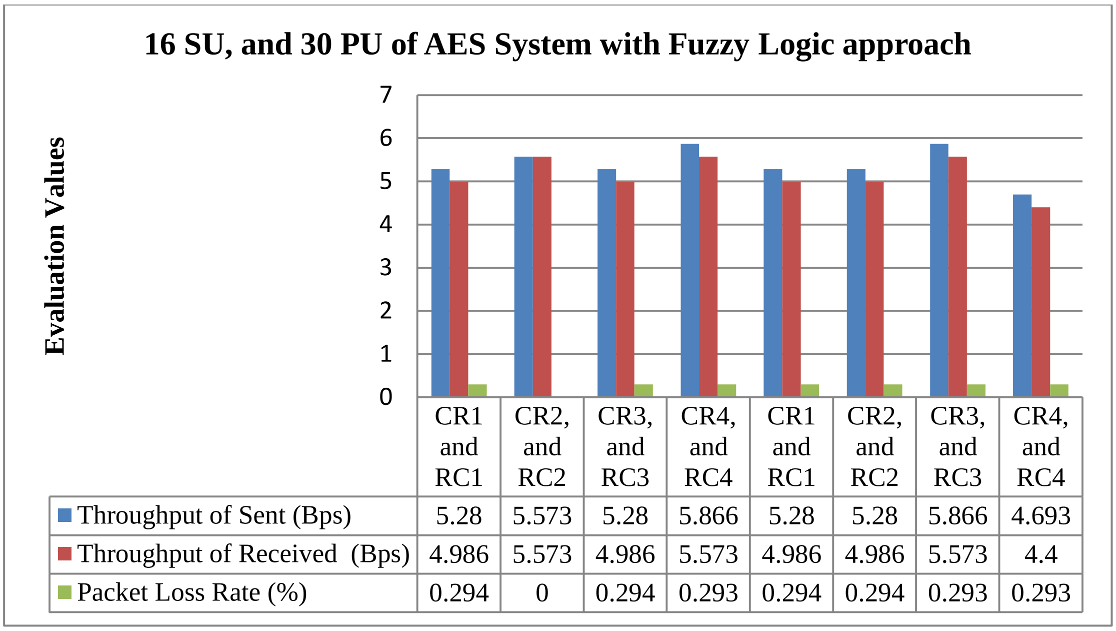
The suggested employment of fuzzy interference serves to enumerate the level of interference caused by the secondary user, thereby facilitating the determination of whether a hand-off is required or not. The utilization of fuzzy interference system in conjunction with channel allocation in cognitive radio results in a decrease in the frequency of switching by secondary users and an enhancement of the general efficiency of both the CRN and the secondary users.

Table 4.8. PDR increases due to the available channel used for transmission is increased after applying fuzzy logic approach to channel allocation.

Table 4.8: Throughput of encapsulated/decapsulated, and Packet Loss Rate of 16 SUs, and 30 PUs in AES case study with Fuzzy Logic approach.

Network Elements		**Payload Throughput / Bps (Encapsulated/Decapsulated)**		**Packet Loss Rate (%)**	**PDR**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	5.28	4.986	0.294	94.4318%
CR 2	RC2	5.573	5.573	0	100%
CR 3	RC3	5.28	4.986	0.294	94.4318%
CR 4	RC4	5.866	5.573	0.293	95.0051%
CR 5	RC5	5.28	4.986	0.294	94.4318%
CR 6	RC6	5.28	4.986	0.294	94.4318%
CR 7	RC7	5.866	5.573	0.293	95.0051%
CR 8	RC8	4.693	4.4	0.293	93.7567%
Data signal size		88 Byte			

Figure 4.4 showed the 16 SU, and 30 PU of AES system with fuzzy logic approach. The total sum of throughput sent packets is 43.118 Bps, the total sum of throughput received packets is 41.063 Bps and the lost packets is 2.055 %. Throughput of sent and received is increased compared with the case of without fuzzy logic with the same numbers of secondary and primary due to the channel allocation enhancement with increased idle channels. Fuzzy model is used to increased chance to get primary user channel by the secondary user node. It improve channel allocation for each cognitive node.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	5.28	5.573	5.28	5.866	5.28	5.28	5.866	4.693
🟥 Throughput of Received (Bps)	4.986	5.573	4.986	5.573	4.986	4.986	5.573	4.4
🟩 Packet Loss Rate (%)	0.294	0	0.294	0.293	0.294	0.294	0.293	0.293

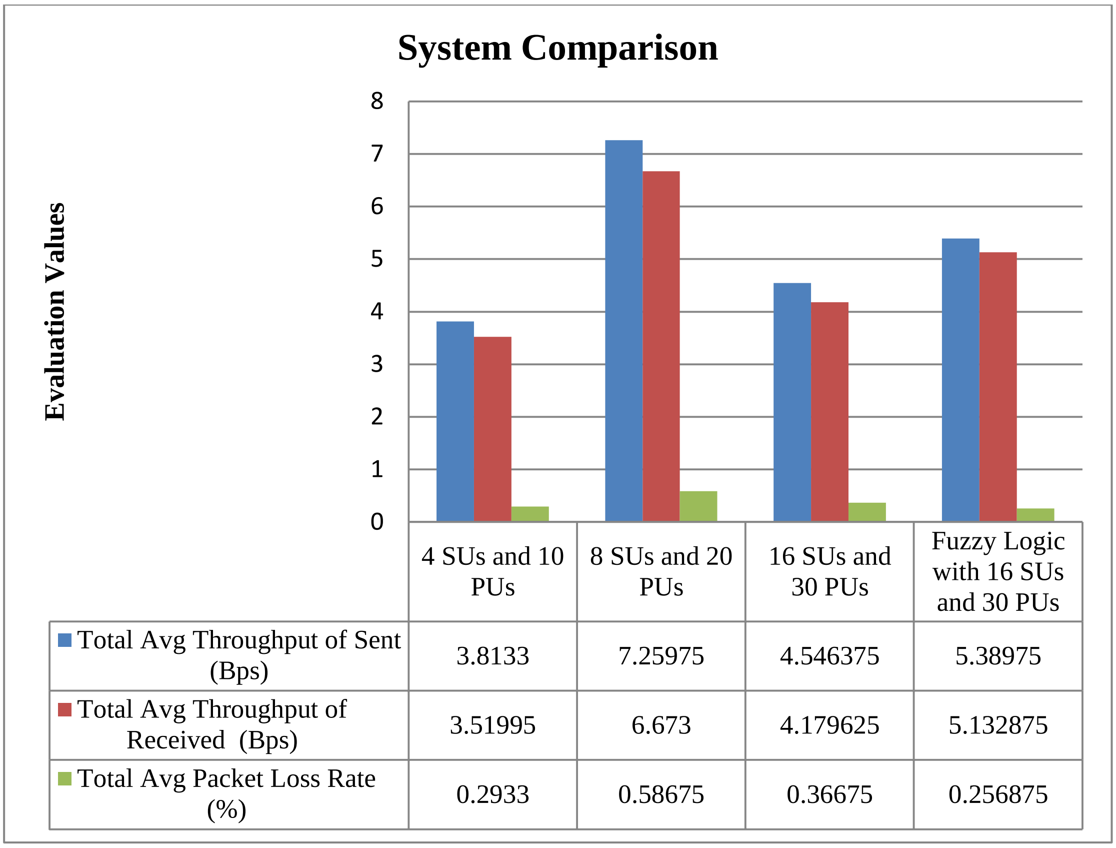
Figure 4.4: Sent, and Received throughput and packet loss rate of 16 SUs, and 30 PUs in AES case study with Fuzzy Logic approach.

Furthermore, Table 4.9 presented the quantity of transmitted and received packets in case of security system with AES encryption algorithm with Fuzzy Logic approach.

Table 4.9: Number of sent/received packets, loss packets of 16 SUs, and 30 PUs in AES case study with Fuzzy Logic approach.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	18	17	1
CR 2	RC2	19	19	0
CR 3	RC3	18	17	1
CR 4	RC4	20	19	1
CR 5	RC5	18	17	1
CR 6	RC6	18	17	1
CR 7	RC7	20	19	1
CR 8	RC8	16	15	1

Figure 4.5 showed the total average of sent and received throughput and average packet loss rate of in AES case study which effects with increased size of data packets entred due to increased number of packets size with AES. The fuzzy logic approach enhanced channel allocation which effects on bandwidth spectrum so the throughput is increased inspite of total number of secondary users increased.



	4 SUs and 10 PUs	8 SUs and 20 PUs	16 SUs and 30 PUs	Fuzzy Logic with 16 SUs and 30 PUs
🟦 Total Avg Throughput of Sent (Bps)	3.8133	7.25975	4.546375	5.38975
🟥 Total Avg Throughput of Received (Bps)	3.51995	6.673	4.179625	5.132875
🟩 Total Avg Packet Loss Rate (%)	0.2933	0.58675	0.36675	0.256875

Figure 4.5: Total average of Sent, and Received throughput and average packet loss rate of in AES case study.

4.2.2 The RC5 security algorithm in CRNs

In this case the proposed system is based on the security encryption data signals with RC5 to encrypt block of data message which passes to the main interface of OMNET++ as 30 Byte of RC5 cipher-text. It is based on the three main cases which are : The 1st case with 4 SUs and 10 PUs; the second case is 8 SUs and 20 PUs; and the 3rd is 16 SUs, and 30 PUs.

4.2.2.1 The case of 4 SUs, and 10 PUs in RC5 security system

It represented by encrypting data signals with RC5 algorithm for the transmit signal among CRN nodes, in addition to the network evaluation parameters showed in Table 4.10.

Table 4.10: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 4 SUs, and 10 PUs in RC5 case study.

Network Elements		**Payload Throughput / Bps (Encapsulated/Decapsulated)**		**Packet Loss Rate (%)**	**PDR %**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	4.2	4.0	0.20	95.2381%
CR 2	RC2	3.7	3.4	0.30	91.8919 %
Data signal size		30 Byte			

The total sum of throughput sent packets is 7.9 Bps, the total sum of throughput received packets is 7.4 Bps and the lost packets is 2.055 %. The data size is decreased compared with AES due to the size of cipher is decreased

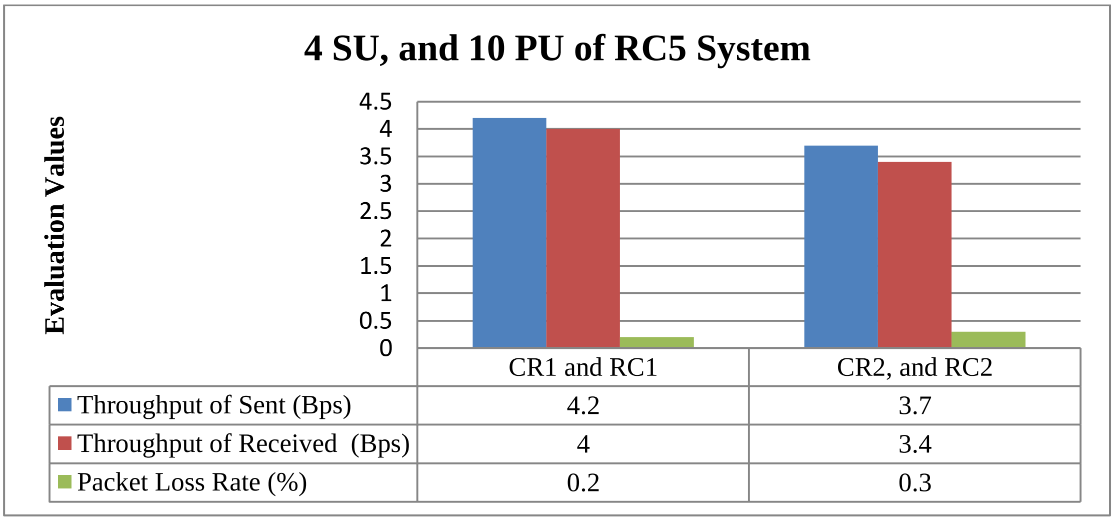


Figure 4.6 : Sent, and Received throughput and packet loss rate of 4SUs, and 10 PUs in RC5 case study.

Table 4.11: Number of sent/received packets, loss packets of 4 SUs, and 10 PUs in RC5 case study.

Network Elements		No. of Packets		No. of Packet Loss
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	42	40	2
CR 2	RC2	37	34	3

4.2.2.2 The case of 8 SU, and 20 PU in RC5 security system

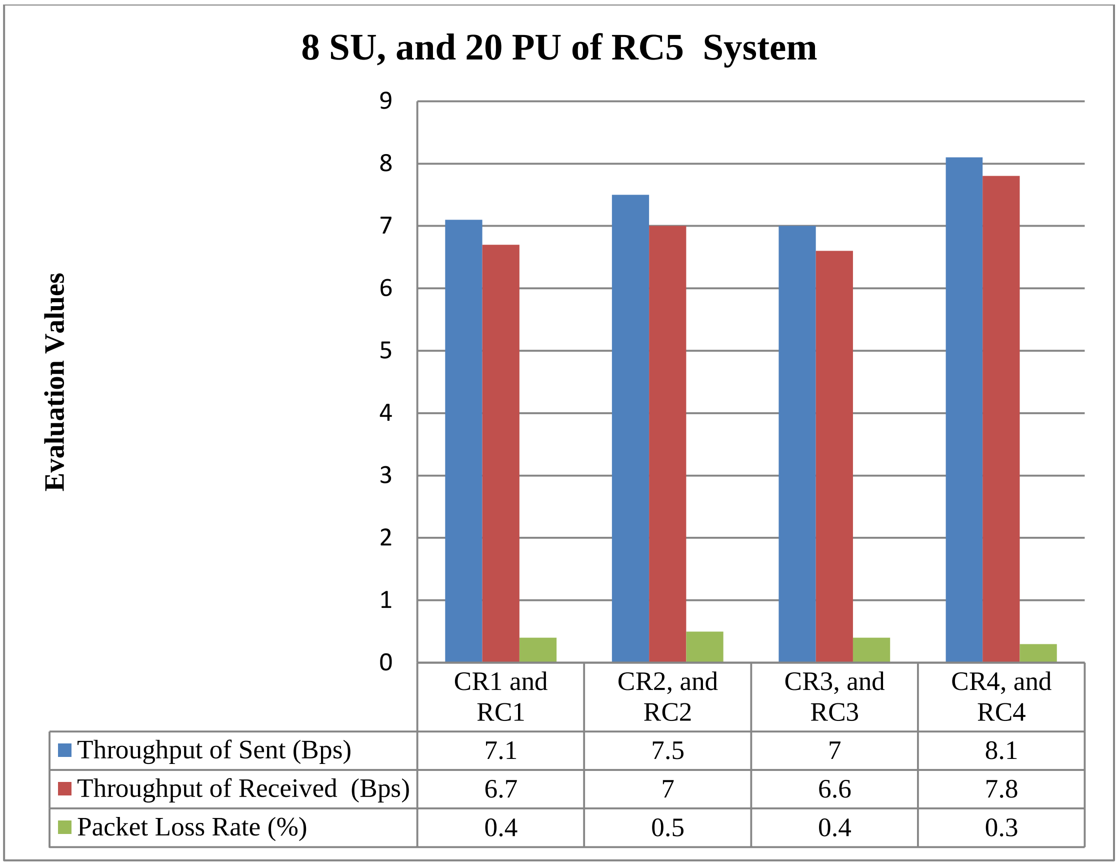
It is applied based on 4 sender and 4 receiver cognitive radio node to exchange RC5 block data signals among CRNs, the evaluation metrics are in Table 4.12.

Table 4.12: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 8 SUs, and 20 PUs in RC5 case study.

Network Elements		Payload Throughput / Bps (Encapsulated/Decapsulated)		Packet Loss Rate (%)	PDR %
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	7.1	6.7	0.4	94.3662%
CR 2	RC2	7.5	7	0.5	93.3333%
CR 3	RC3	7	6.6	0.4	94.2857%
CR 4	RC4	8.1	7.8	0.3	96.2963%
Data signal size		30 Byte			

Figure 4.7 showed the increased throughput of sender and receiver due to the increased number of nodes which effects on created packets for each device. The total sum of throughput sent packets is 29.7 Bps, the total sum of throughput received packets is 28.1 Bps and the lost packets is 1.6 %. Throughput is increased due to the number of sent

packets is increased in case of RC5 compared with the same number of packets from AES algorithm.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	7.1	7.5	7	8.1
🟥 Throughput of Received (Bps)	6.7	7	6.6	7.8
🟩 Packet Loss Rate (%)	0.4	0.5	0.4	0.3

Figure 4.7 : Sent, and Received throughput and packet loss rate of 8 SUs, and 20 PUs in RC5 case study.

Table 4.13: Number of sent/received packets, loss packets of 8 SUs, and 20 PUs in RC5 case study.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	71	67	4
CR 2	RC2	75	70	5
CR 3	RC3	70	666	4
CR 4	RC4	81	78	3

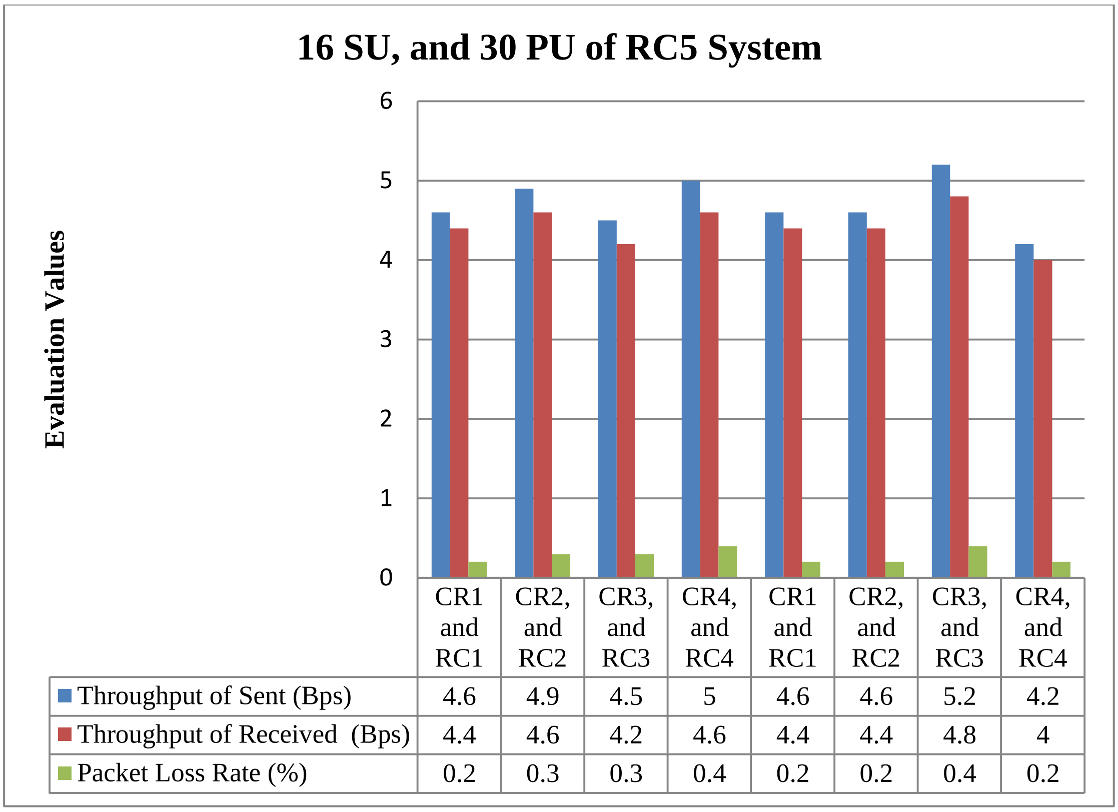
4.2.2.3 The case of 16 SUs, and 30 PUs in RC5 security system

In this case, the number of cognitive radio nodes increases, and the network evaluation metrics are affected as presented in Table 4.14 and Figure 4.8, respectively.

Table 4.14: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 16 SUs, and 30 PUs in RC5 case study.

Network Elements		**Payload Throughput / Bps (Encapsulated/Decapsulated)**		**Packet Loss Rate (%)**	**PDR %**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	4.6	4.4	0.2	95.6522%
CR 2	RC2	4.9	4.6	0.3	93.8776%
CR 3	RC3	4.5	4.2	0.3	93.3333%
CR 4	RC4	5	4.6	0.4	0.92%
CR 5	RC5	4.6	4.4	0.2	95.6522%
CR 6	RC6	4.6	4.4	0.2	95.6522%
CR 7	RC7	5.2	4.8	0.4	92.3077%
CR 8	RC8	4.2	4	0.2	95.2381%
Data signal size		30 Byte			

Figure 4.8 showed the total sum of throughput sent packets is 37.6 Bps, the total sum of throughput received packets is 35.4 Bps and the lost packets is 2.2 %. Throughput of RC5 is increased due to the size of data message is less than AES case study, besides lost packets is decreased due to the total number of received packets is increased during period time of execution.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	4.6	4.9	4.5	5	4.6	4.6	5.2	4.2
🟥 Throughput of Received (Bps)	4.4	4.6	4.2	4.6	4.4	4.4	4.8	4
🟩 Packet Loss Rate (%)	0.2	0.3	0.3	0.4	0.2	0.2	0.4	0.2

Figure 4.8: Sent, and Received throughput and packet loss rate of 16 SUs, and 30 PUs in RC5 case study.

Table 4.15 showed the sent/received packets, loss packets of 16 SUs, and 30 PUs in RC5 case study. It is the best compared with AES due to the size of packets in AES is bigger than of RC5.

Table 4.15: Number of sent/received packets, loss packets of 16 SUs, and 30 PUs in RC5 case study.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	46	44	2
CR 2	RC2	49	46	3
CR 3	RC3	45	42	3
CR 4	RC4	50	46	4
CR 5	RC5	46	44	2

CR 6	RC6	46	44	2
CR 7	RC7	52	48	4
CR 8	RC8	42	40	2

4.2.2.4 The case of 16 SUs, and 30 PUs in RC5 security system with Fuzzy Logic Approach

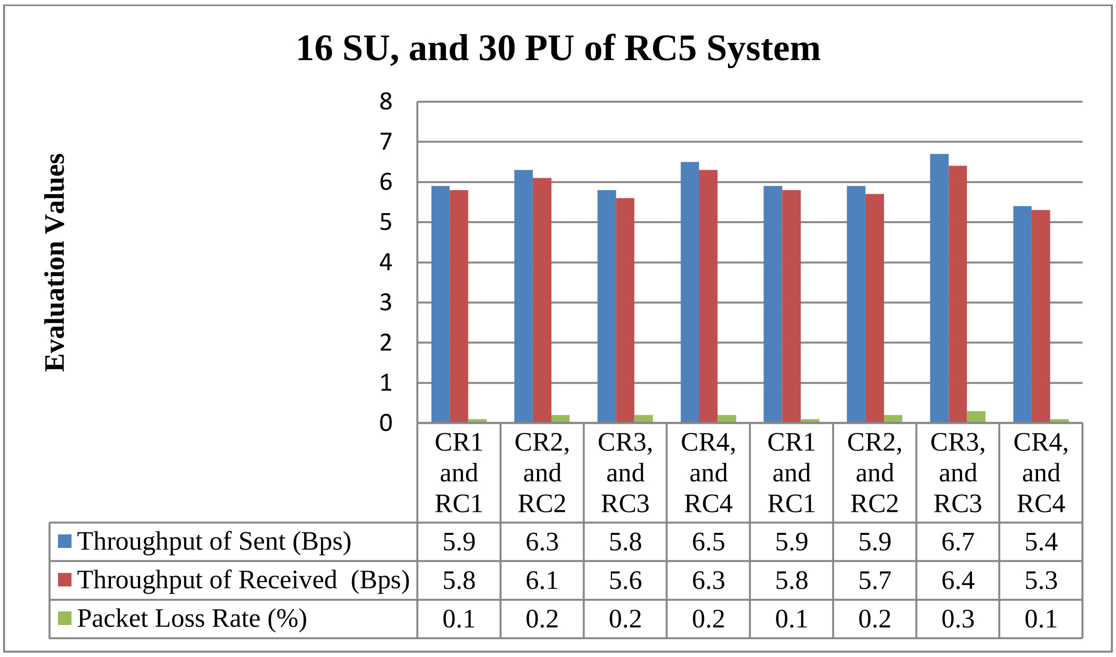
The proposed fuzzy logic improves the sensing state of cognitive radio network by decreasing the number of sensing signals through primary user behavior, each cognitive radio sense the channel with primary user signal detector to make a decision about the best idle channel shared among nodes in cognitive cycle. Table 4.16, and Figure 4.9 show the evaluation metrics of this case study. It showed the throughput and PDR in increased due to increase total number of packets arrived without error because of maximize total number of idle primary user channel after applying fuzzy logic resource channel allocation which managed channel allocation with secondary user.

Table 4.16: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 16 SUs, and 30 PUs in RC5 case study.

Network Elements		**Payload Throughput / Bps (Encapsulated/Decapsulated)**		**Packet Loss Rate (%)**	**PDR%**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	5.9	5.8	0.1	98.3051%
CR 2	RC2	6.3	6.1	0.2	96.8254%
CR 3	RC3	5.8	5.6	0.2	96.5517%
CR 4	RC4	6.5	6.3	0.2	96.9231%
CR 5	RC5	5.9	5.8	0.1	98.3051%
CR 6	RC6	5.9	5.7	0.2	96.6102%

CR 7	RC7	6.7	6.4	0.3	95.5224%
CR 8	RC8	5.4	5.3	0.1	98.1481%
Data signal size		30 Byte			

The total sum of throughput sent packets is 48.4 Bps, the total sum of throughput received packets is 47 Bps and the lost packets is 1.4 %. Throughput is increased in case of RC5 compared with the case of AES with the same number of secondary and primary nodes due to the size of data message of RC5 is less than AES.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	5.9	6.3	5.8	6.5	5.9	5.9	6.7	5.4
🟥 Throughput of Received (Bps)	5.8	6.1	5.6	6.3	5.8	5.7	6.4	5.3
🟩 Packet Loss Rate (%)	0.1	0.2	0.2	0.2	0.1	0.2	0.3	0.1

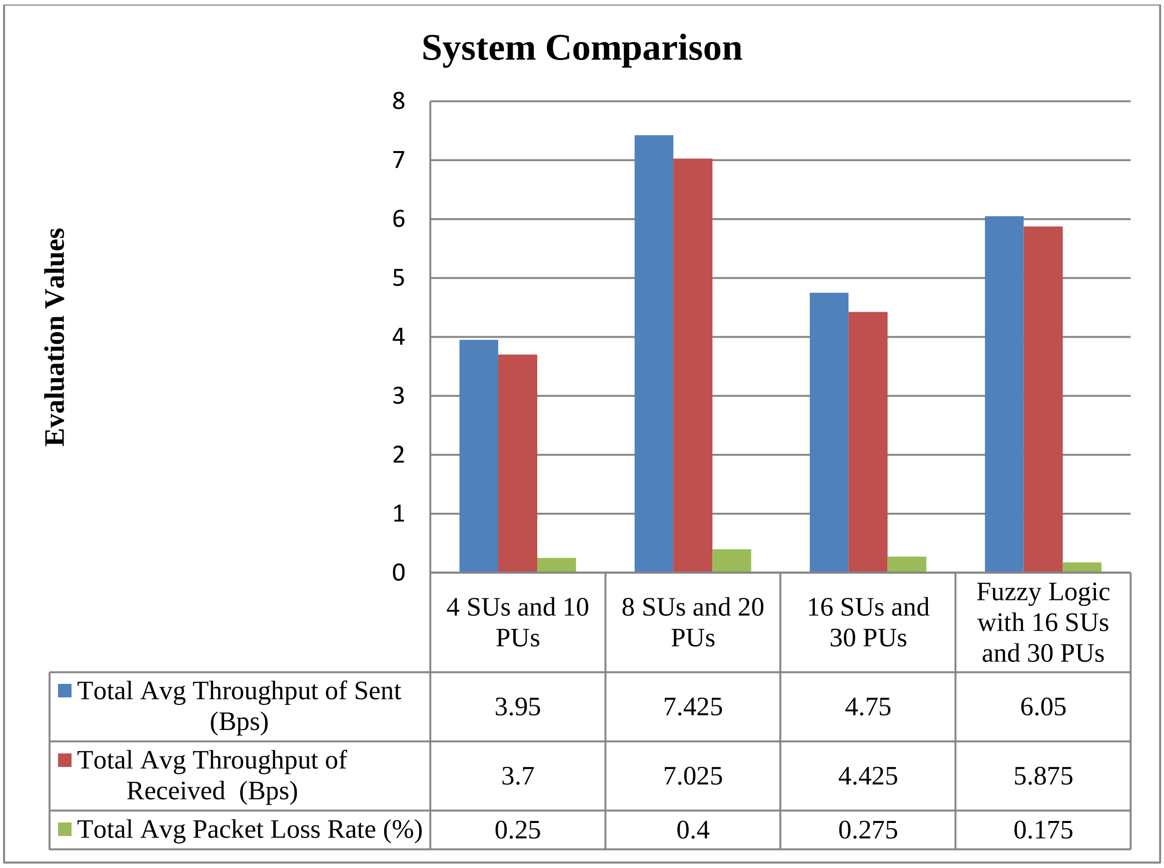
Figure 4.9: Sent, and Received throughput and packet loss rate of 16 SUs, and 30 PUs in RC5 case study.

Table 4.17: Number of sent/received packets, loss packets of 16 SUs, and 30 PUs in RC5 case study.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	59	58	1
CR 2	RC2	63	61	2

CR 3	RC3	58	56	2
CR 4	RC4	65	63	2
CR 5	RC5	59	58	1
CR 6	RC6	59	57	2
CR 7	RC7	67	64	3
CR 8	RC8	54	53	1

Figure 4.10 showed the throughput enhancement for sent and received due to the channel allocation management with fuzzy logic approach which controlled on primary channel selection for each secondary user to get access to the idle primary user channel which effects on bandwidth spectrum.



	4 SUs and 10 PUs	8 SUs and 20 PUs	16 SUs and 30 PUs	Fuzzy Logic with 16 SUs and 30 PUs
🟦 Total Avg Throughput of Sent (Bps)	3.95	7.425	4.75	6.05
🟥 Total Avg Throughput of Received (Bps)	3.7	7.025	4.425	5.875
🟩 Total Avg Packet Loss Rate (%)	0.25	0.4	0.275	0.175

Figure 4.10: Total average of Sent, and Received throughput and average packet loss rate of in RC5 case study.

4.2.3 The normal cognitive radio system (without security algorithm)

It is implemented with binary block of data signals passed among cognitive radio signals. This case is represented without any security system to simulate data signals exchange among cognitive radio nodes. It is based on the 4th of case studies : 4 SUs and 10 PUs; 8 SUs and 20 PUs ; and 16 SUs and 30 PUs.

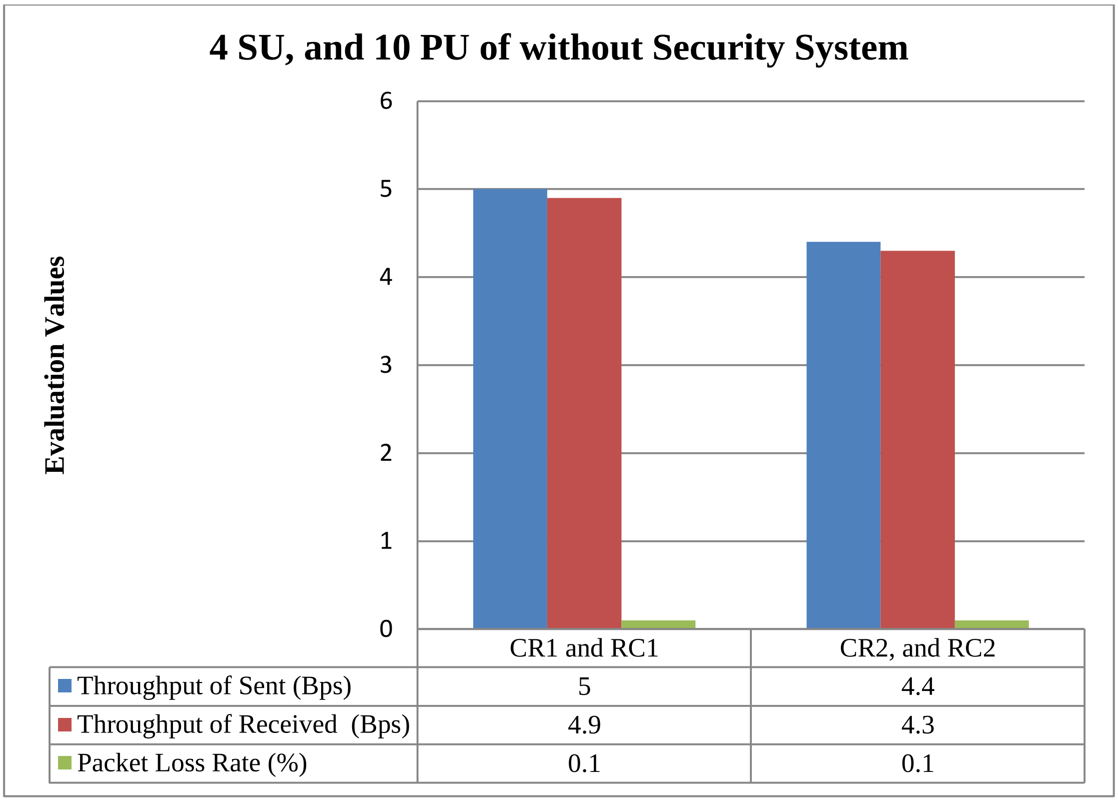
4.2.3.1 The case of 4 SUs, and 10 PUs in cognitive radio network

Table 4.18 shows the throughput and packet loss rate of this case study with the maximum data signals size ; 30 byte of binary series.

Table 4.18: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 4 SUs, and 10 PUs in case study of without security system.

Network Elements		**Payload Throughput / Bps**		**Packet Loss Rate (%)**	**PDR %**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	5	4.9	0.1	98%
CR 2	RC2	4.4	4.3	0.1	97.7273%
Data signal size		30 Byte			

Figure 4.11 showed the 4 SU, and 10 PU of without security system. The total sum of throughput sent packets is 9.4 Bps, the total sum of throughput received packets is 9.2 Bps and the lost packets is 0.2 %. Throughput is better compared with two case studies AES and RC5 due to the size of data is less than from both and data required time to transmit cipher text is larger than required time to send clear plain text.



	CR1 and RC1	CR2, and RC2
🟦 Throughput of Sent (Bps)	5	4.4
🟥 Throughput of Received (Bps)	4.9	4.3
🟩 Packet Loss Rate (%)	0.1	0.1

Figure 4.11 : Sent, and Received throughput and packet loss rate of 4SUs, and 10 PUs in case study of without security system.

Table 4.19: Number of sent/received packets, loss packets of 4 SUs, and 10 PUs in case study of without security system.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	50	49	1
CR 2	RC2	44	43	1

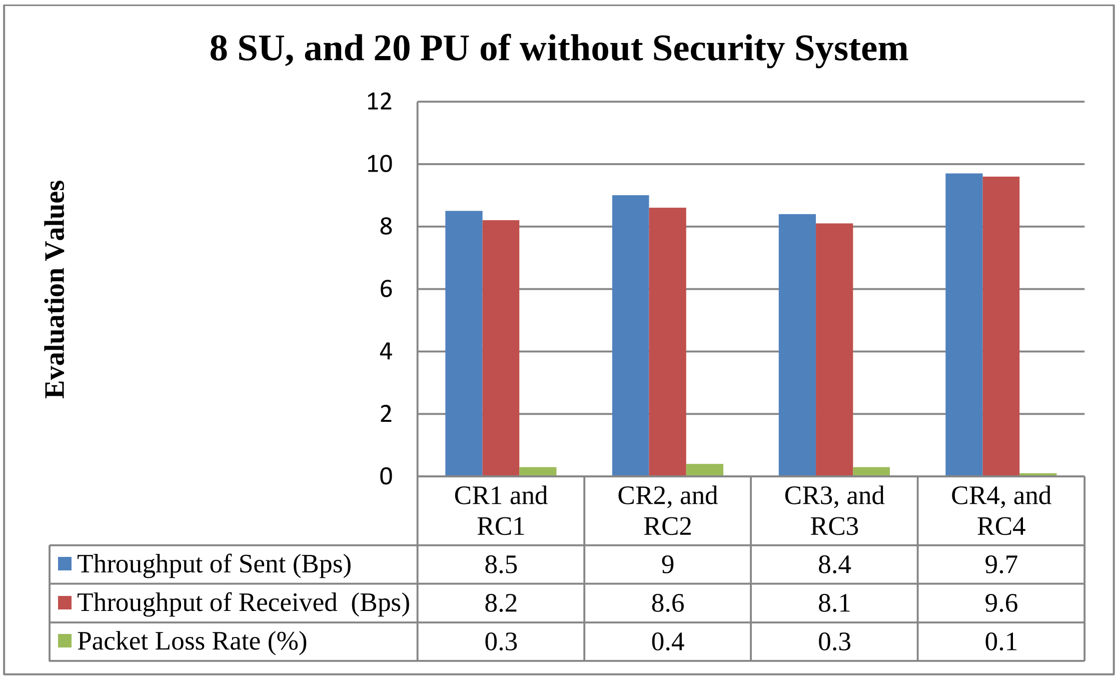
4.2.3.2 The case of 8 SUs, and 20 PUs in cognitive radio network

In this case, the proposed system is implemented without any features for security purpose as normal system. It shows open channel for transmission without checkpoint or filtration points ; also, the size of data is less that in case of security system, so PDR is high and packet loss rate is low.

Table 4.20: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 8 SUs, and 20 PUs in case study of without security system.

Network Elements		**Payload Throughput / Bps**		**Packet Loss Rate (%)**	**PDR %**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	8.5	8.2	0.3	96.4706%
CR 2	RC2	9	8.6	0.4	95.5556%
CR 3	RC3	8.4	8.1	0.3	96.4286%
CR 4	RC4	9.7	9.6	0.1	98.9691%
Data signal size		30 Byte			

Figure 4.12 showed 8 SU, and 20 PU of without security system, throughput with increased number of secondary users is creased due to increased waiting time and overloading to choice best idle primary user channel. The total sum of throughput sent packets is 35.6 Bps, the total sum of throughput received packets is 34.5 Bps and the lost packets is 1.1 %.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	8.5	9	8.4	9.7
🟥 Throughput of Received (Bps)	8.2	8.6	8.1	9.6
🟩 Packet Loss Rate (%)	0.3	0.4	0.3	0.1

Figure 4.12 : Sent, and Received throughput and packet loss rate of 8 SUs, and 20 PUs in cognitive radio network case study.

Table 4.21: Number of sent/received packets, loss packets of 8 SUs, and 20 PUs in case study of without security system.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	85	82	3
CR 2	RC2	90	86	4
CR 3	RC3	84	81	3
CR 4	RC4	97	96	1

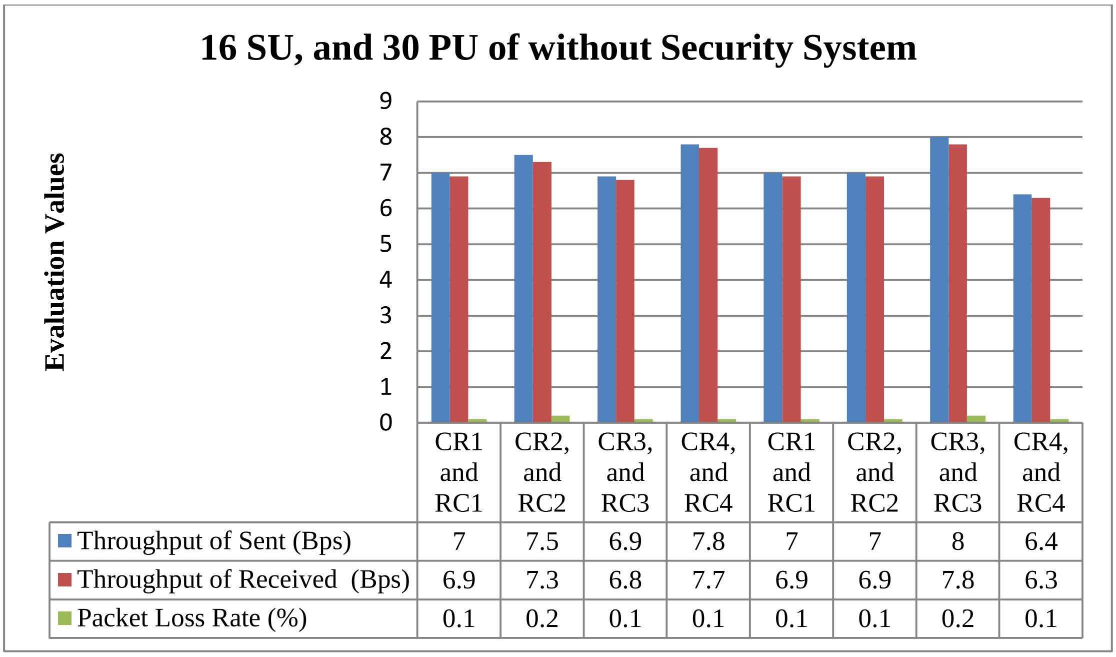
4.2.3.3 The case of 16 SU, and 30 PU in cognitive radio network

This case showed payload throughput is effected with the increased number of secondary user and primary user so it is decreased with increased number of secondary user.

Table 4.22: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 16 SUs, and 30 PUs in case study of without security system.

Network Elements		**Payload Throughput / Bps**		**Packet Loss Rate (%)**	**PDR**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	7	6.9	0.1	98.5714%
CR 2	RC2	7.5	7.3	0.2	97.3333%
CR 3	RC3	6.9	6.8	0.1	98.5507%
CR 4	RC4	7.8	7.7	0.1	98.7179%
CR 5	RC5	7	6.9	0.1	98.5714%
CR 6	RC6	7	6.9	0.1	98.5714%
CR 7	RC7	8	7.8	0.2	97.5%
CR 8	RC8	6.4	6.3	0.1	98.4375%
Data signal size		30 Byte			

Figure 4.13 showed the 16 SU, and 30 PU of without security system. The total sum of throughput sent packets is 57.6 Bps, the total sum of throughput received packets is 56.6 Bps and the lost packets is 1 %. Throughput is the best compared with AES and RC5 with the same number of nodes due to the data message is less and required time to pass data from sender to the receiver is less.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	7	7.5	6.9	7.8	7	7	8	6.4
🟥 Throughput of Received (Bps)	6.9	7.3	6.8	7.7	6.9	6.9	7.8	6.3
🟩 Packet Loss Rate (%)	0.1	0.2	0.1	0.1	0.1	0.1	0.2	0.1

Figure 4.13: Sent, and Received throughput and packet loss rate of 16 SUs, and 30 PUs in case study of without security system.

Table 4.23: Number of sent/received packets, loss packets of 16 SUs, and 30 PUs in case study of without security system.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	70	69	1
CR 2	RC2	75	73	2
CR 3	RC3	69	68	1
CR 4	RC4	78	77	1

CR 5	RC5	70	69	1
CR 6	RC6	70	69	1
CR 7	RC7	80	78	2
CR 8	RC8	64	63	1

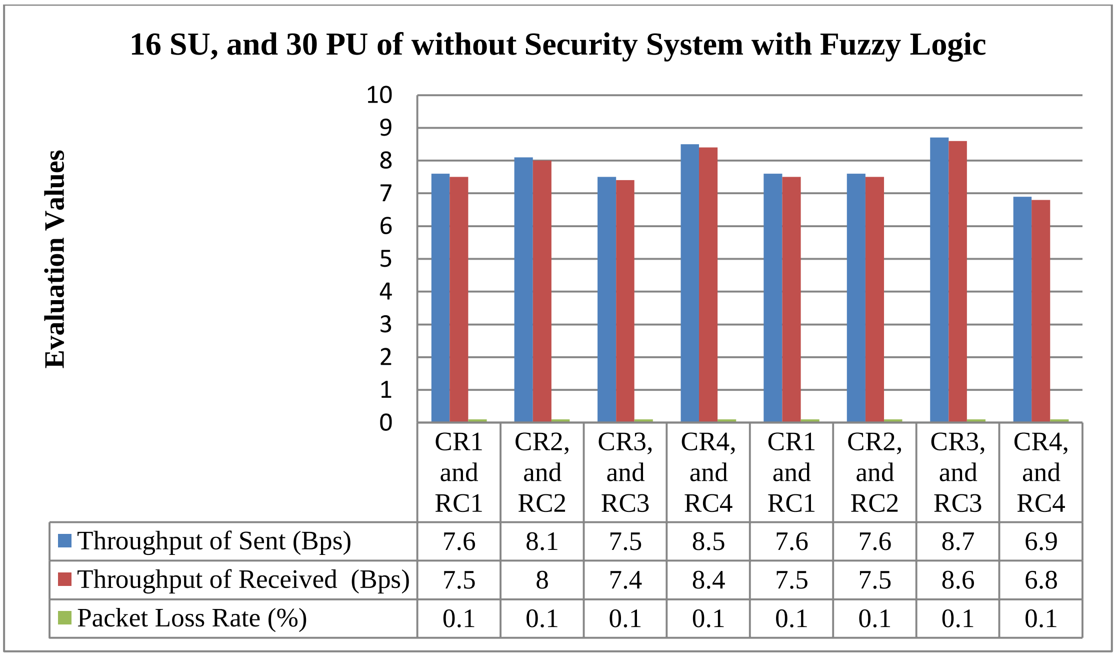
4.2.3.4 The case of 16 SU, and 30 PU in cognitive radio network with Fuzzy Logic approach

The main purpose of fuzzy logic approach is to improve network performance and to enhance throughput by selecting optimal channel and decreasing the number of required sensing message to left channel through primary user appearance. The fuzzy logic approach is used in case of maximum secondary users as showed in Table 4.24.

Table 4.24: Payload throughput of encapsulated/decapsulated, and Packet Loss Rate of 16 SUs, and 30 PUs in case study without security system with fuzzy logic.

Network Elements		**Payload Throughput / Bps**		**Packet Loss Rate (%)**	**PDR %**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
CR 1	RC1	7.6	7.5	0.1	98.6842%
CR 2	RC2	8.1	8	0.1	98.7654%
CR 3	RC3	7.5	7.4	0.1	98.6667%
CR 4	RC4	8.5	8.4	0.1	98.8235%
CR 5	RC5	7.6	7.5	0.1	98.6842%
CR 6	RC6	7.6	7.5	0.1	98.6842%
CR 7	RC7	8.7	8.6	0.1	98.8506%
CR 8	RC8	6.9	6.8	0.1	98.5507%
Data signal size		30 Byte			

Figure 4.14 showed the total sum of throughput sent packets is 62.5 Bps, the total sum of throughput received packets is 61.7 Bps and the lost packets is 0.8 %. Throughput is increased with the case of using fuzzy logic due to the improvement of channel allocation by fuzzy model which effect on total number of idle channel of each secondary user.



	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4	CR1 and RC1	CR2, and RC2	CR3, and RC3	CR4, and RC4
🟦 Throughput of Sent (Bps)	7.6	8.1	7.5	8.5	7.6	7.6	8.7	6.9
🟥 Throughput of Received (Bps)	7.5	8	7.4	8.4	7.5	7.5	8.6	6.8
🟩 Packet Loss Rate (%)	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1

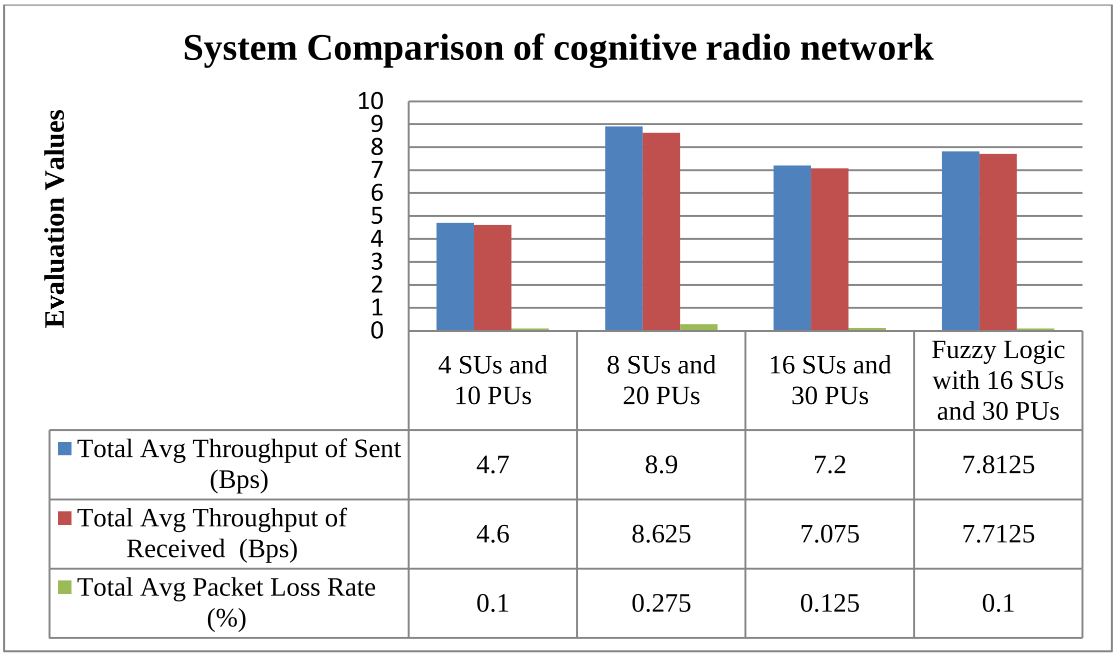
Figure 4.14: Sent, and Received throughput and packet loss rate of 16 SUs, and 30 PUs in case study of without security system with Fuzzy Logic.

Table 4.25: Number of sent/received packets, loss packets of 16 SUs, and 30 PUs in case study of without security system with Fuzzy Logic.

Network Elements		**No. of Packets**		**No. of Packet Loss**
Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**	
CR 1	RC1	76	75	1
CR 2	RC2	81	80	2
CR 3	RC3	75	74	1
CR 4	RC4	85	84	1
CR 5	RC5	76	75	1

CR 6	RC6	76	75	1
CR 7	RC7	87	86	1
CR 8	RC8	69	68	1

Figure 4.15 showed the throughput enhancement in case of fuzzy logic due to the available channel is increased so bandwidth is maximized and lost packets is decreased due to the collision of large number of secondary user is decreased.



	4 SUs and 10 PUs	8 SUs and 20 PUs	16 SUs and 30 PUs	Fuzzy Logic with 16 SUs and 30 PUs
🟦 Total Avg Throughput of Sent (Bps)	4.7	8.9	7.2	7.8125
🟥 Total Avg Throughput of Received (Bps)	4.6	8.625	7.075	7.7125
🟩 Total Avg Packet Loss Rate (%)	0.1	0.275	0.125	0.1

Figure 4.15: Total average of Sent, and Received throughput and average packet loss rate of in cognitive radio network case study with Fuzzy Logic.

4.3 The 2nd security system for cognitive radio network

The 2nd secure system is implemented and tested with other security methods to ensure that it is (in both states) is fixable and applicable to enhance the security side in cognitive radio network. The data used is 20 B Text, 30 KB image file, and 800 KB excel file for environmental data reads. The number of network elements is : 18

Secondary users, and 8 Primary users with CTP for security purposes and one base-station(SUs-BS, PUs-BS) and other network devices.

4.3.1 Security with Authentication ECC algorithm in CRNs

The proposed system is implemented with ECC algorithm which is programmed in C# and the output is used as outside code result library in OMNET++ for key exchange in the used secure CR system. ECC method is used to authenticate these packets. Figure 4.16 showed the authentication process with ECC algorithm.

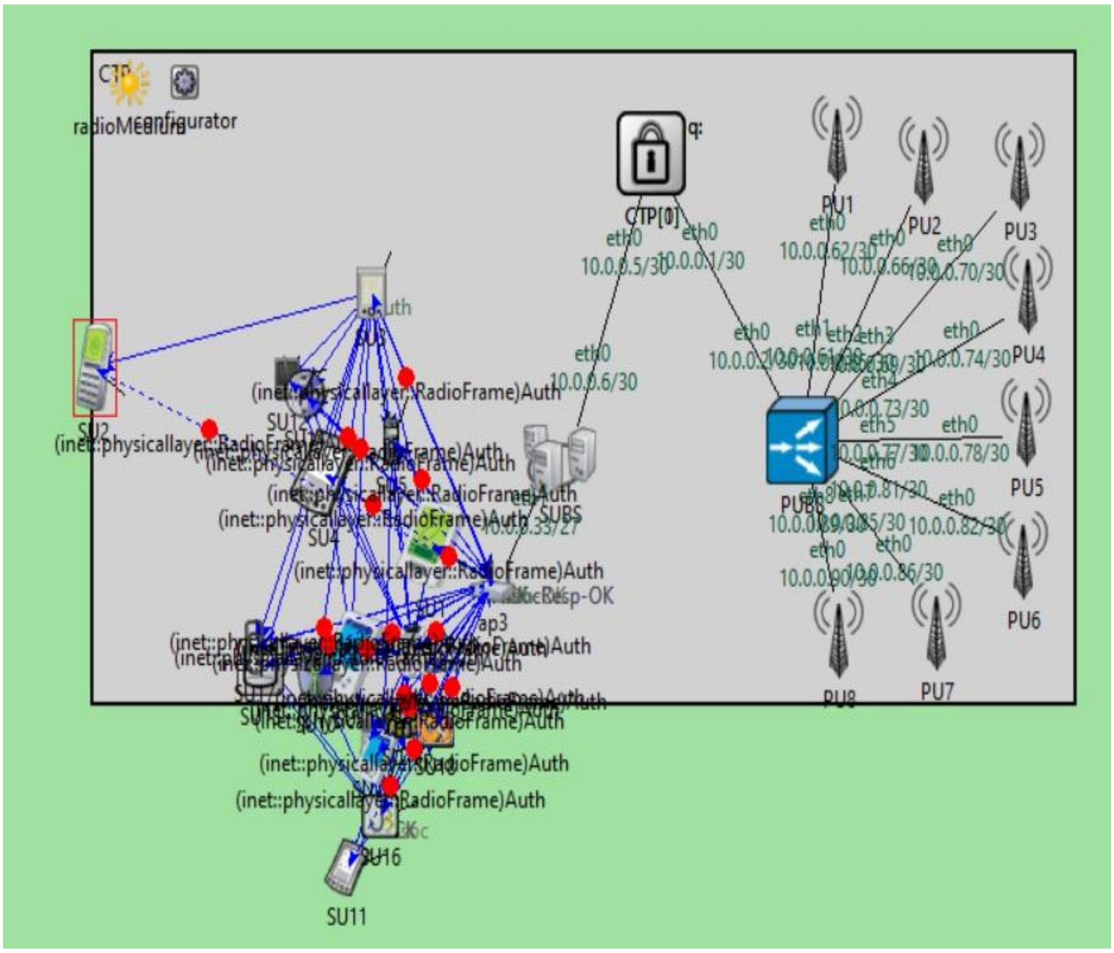


Figure 4.16: ECC algorithm in OMNET++.

Table 4.26 shows the data types with the proposed security cognitive radio system and each size of data type.

Table 4.26: The used data type with the data size.

Data Type	Size
Text Data signal size	20 B
Image Data signal size	30 KB
File Data signal size	800 KB
ECC private/public key size	256 bits
ECC Session Key size	256 bits

The implementation of the ECC algorithm results in enhanced communication time and throughput efficiency. The expeditious transition of the data channel for secure authenticated communication is attributed to the reduced duration of communication over the control channel following the exchange of selected idle channel lists and available channel lists. The authentication process for ECC during the sensing phase operations is executed from the BSs to the CTP node, with the aim of verifying and validating the sensing requests, and then opening the secure channel for data transmission in case of SU-BSs and secure sensing information for channel allocation from PU-BSs. The used ECC public/private keys are employed, and Session key is 256 bits. Table 4.27 shows the results of this case study.

Table 4.27: Security with Authentication ECC algorithm in CRNs

Data Type	**Network Elements**		**Payload Throughput / Bps**		**Probability of Channel Collision**	**PDR %**
	Send Nodes	**Received Nodes**	**Encapsulated Packets/sec Sent**	**De-capsulated Packets/sec Received**		
Text	CR 1	RC2	182.4	181	0.014	99.232 %
	CR 3	RC4	194.5	193	0.042	99.228 %
	CR 5	RC6	180	178.9	0.0028	99.388 %
	CR 7	RC8	331500	327900	0.0182	98.914 %

Image	CR 9	RC10	296400	294500	0.07	99.359 %
	CR 11	RC12	296400	293500	0.014	99.021 %
File	CR 13	RC 14	12528000	12394000	0.112	98.930 %
	CR 15	RC 16	9936000	9872000	0.168	99.355 %
	CR 17	CR 18	10656000	10568000	0.21	99.174 %

4.3.2 Security with Integrity SHA-3 algorithm in CRNs

The SHA-3 hash function, as proposed, offers data integrity by producing a distinct hash digest in response to any minor or major alteration in the data. Consequently, they are frequently employed to ascertain the presence or absence of data tampering. It is programmed with C# and the output added to the packet fields is in the OMNET++. Furthermore, the algorithm offers collision resistance and generates a hashed value of a predetermined length of 288 bits. The algorithm's construction is based on an iterative (cascaded) approach. Figure 4.17 shows SHA-3 integrity in OMNET++.

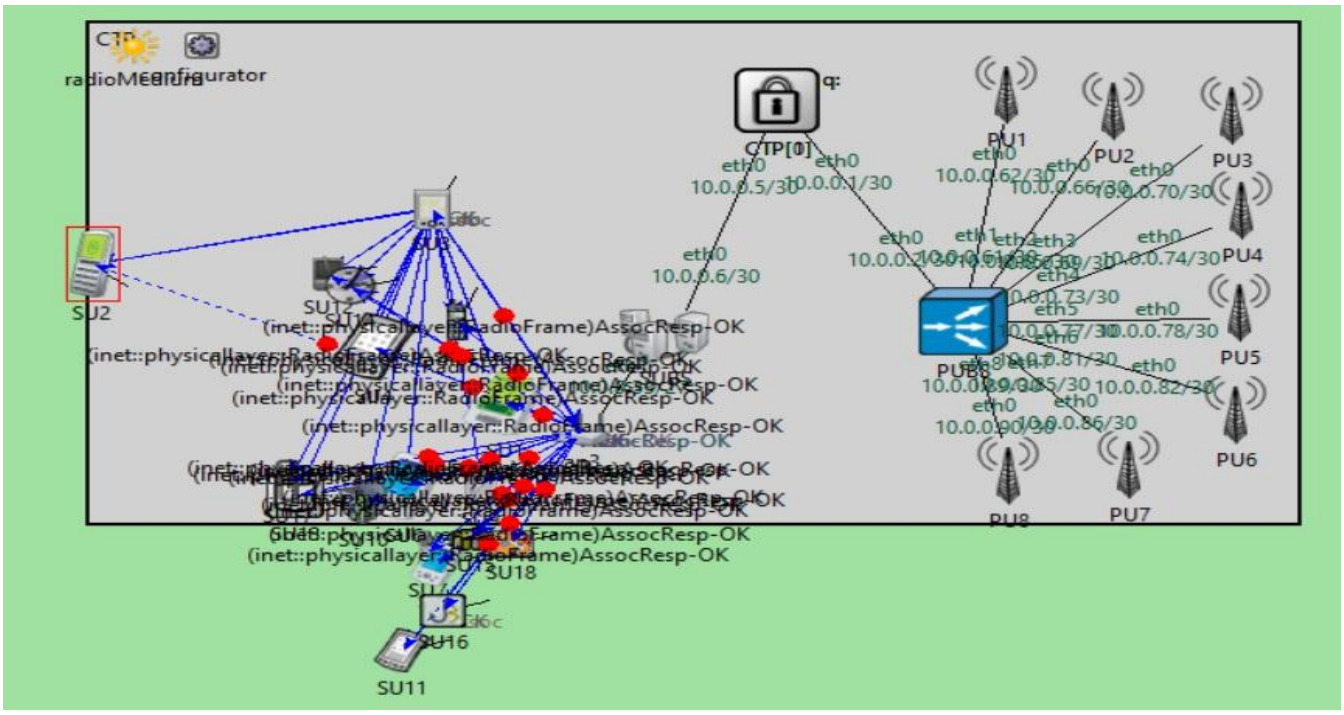


Figure 4.17: Data integrity proved in the SHA-3 system case study.

Furthermore, to mitigate algorithmic complexity and lengthy processing times in CRN applications, a keyless hash algorithm is employed. The processing stage encompasses three key steps, namely message padding, splitting the padded message into blocks of 512 bits, and establishing initial vectors for use in the subsequent phase. The subsequent stage involves the computation of the hash, which encompasses message time management, round functions, word operations, and constants that are utilized in a repetitive manner to generate the ultimate hash value, which is 288 bits in length. Table 4.28 shows the integrity with SHA-3 security system results. Probability of channel collision is decreased compared to the case of authentication because the required time of integrity is less than the required time of authentication; besides PDR increases due to the increasing successful packets arriving to the destination secondary user.

Table 4.28: Security with Integrity SHA-3 algorithm in CRNs

Data Type	Network Elements		Payload Throughput / Bps		Probability of Channel Collision	PDR %
	Send Nodes	Received Nodes	Encapsulated Packets/sec Sent	De-capsulated Packets/sec Received		
Text	CR 1	RC2	136.8	136.13	0.011	99.510 %
	CR 3	RC4	145.875	144.89	0.033	99.324 %
	CR 5	RC6	135	134.597	0.0022	99.701 %
Image	CR 7	RC8	248625	248367	0.0143	99.896 %
	CR 9	RC10	222300	221985	0.055	99.858 %
	CR 11	RC12	222300	221255	0.011	99.529 %
File	CR 13	RC 14	9396000	9387620	0.088	99.910 %
	CR 15	RC 16	7452000	7446560	0.132	99.927 %
	CR 17	CR 18	7992000	7974640	0.165	99.782 %

4.3.3 Security with Authentication ECC and Integrity SHA-3 algorithms in CRNs

The integrated security system under consideration offers a dependable and effective cognitive radio setting by leveraging the ECC and SHA-3 algorithms. The objective is to sustain the integrity of the entire network and enhance its resilience against potential hazards that may specifically target the designated authentication nodes. The SUs-BSs and PUs-BSs that are registered have the ability to communicate and create a necessary session key through employment of the ECC algorithm. This algorithm is exclusive to the particular pair of SUs and PUs involved in a given communication. The resulting session key will be utilized to ensure the security of their communication throughout the connection session. Figure 4.18, Figure 4.19 and Figure 4.20 show the integrated system results with channel free to verify and be redirected to CTP, then to secondary user base station.

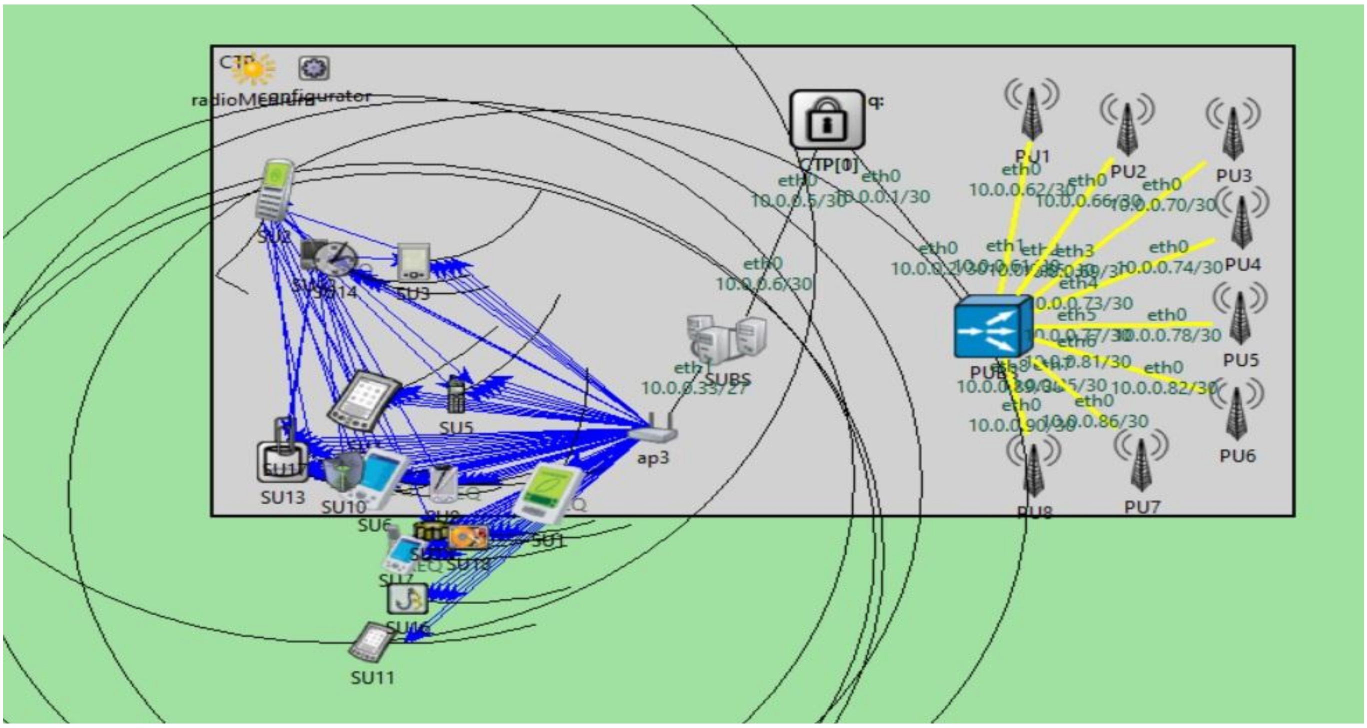


Figure 4.18 : Primary user channel allocation with Base station (PU-BS).

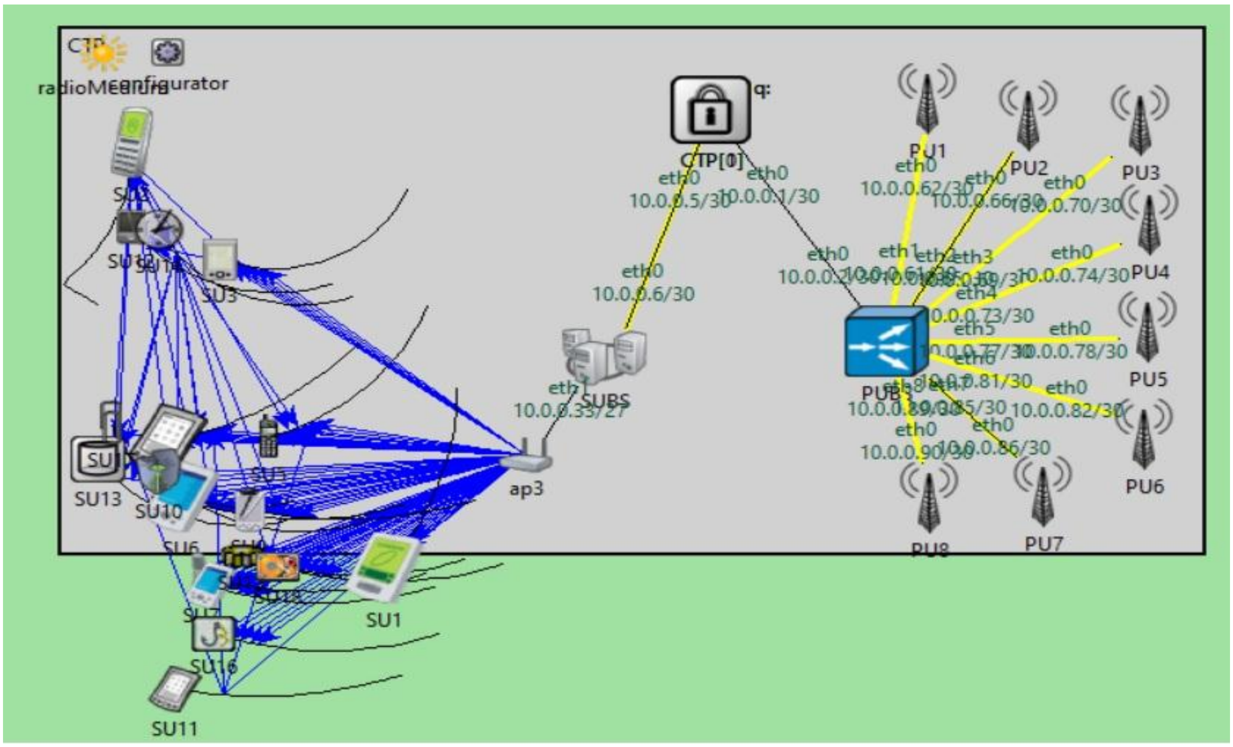


Figure 4.19 : Selected channel idle and redirect to BS-SUs.

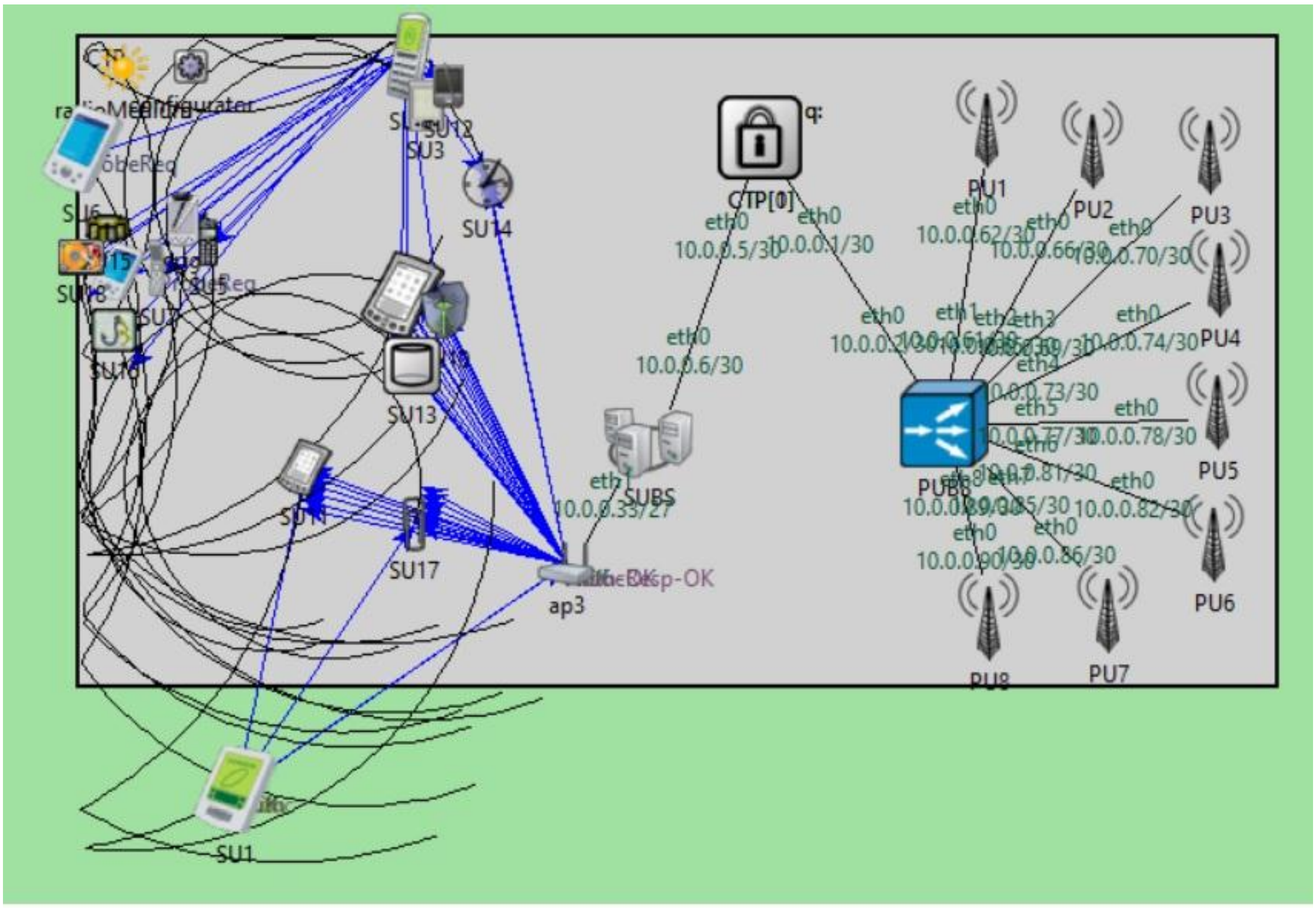


Figure 4.20: Data proved and verified secure connection.

The utilization of an integrated system results in a reduction in the quantity of security-related frames that are exchanged between SUs. Additionally, the CTP is employed to authenticate cognitive users and facilitate the establishment of a secure session key between a pair of BSs to ensure the security of their communication. The ECC algorithm generates a security session key of greater size, which results in a heightened level of security with data integrity SHA-3 algorithm in the proposed security system. PDR increases due to the increasing number of successful packets acknowledged from the destination secondary user. Table 4.29 shows the security system with authentication ECC and integrity SHA-3 algorithms in CRNs.

Table 4.29: Security with Authentication ECC and Integrity SHA-3 algorithms in CRNs

Data Type	Network Elements		Payload Throughput / Bps		Probability of Channel Collision	PDR %
	Send Nodes	Received Nodes	Encapsulated Packets/sec Sent	De-capsulated Packets/sec Received		
Text	CR 1	RC2	155.04	154.784	0.01	99.834 %
	CR 3	RC4	165.325	164.5263	0.03	99.516 %
	CR 5	RC6	153	152.95	0.002	99.967 %
Image	CR 7	RC8	281775	280998.8	0.013	99.724 %
	CR 9	RC10	251940	251849	0.05	99.963 %
	CR 11	RC12	251940	251149	0.01	99.686 %
File	CR 13	RC 14	10648800	10647480	0.08	99.987 %
	CR 15	RC 16	8445600	8444760	0.12	99.990 %
	CR 17	CR 18	9057600	9048960	0.15	99.904 %

In authentication case with authentication ECC algorithm the total sum of probability of channel Collision is 0.651; total average of PDR is 99.18 %. Besides, the Integrity SHA-3 algorithm is the total sum of probability of channel Collision that is 0.5115; total average of PDR is 99.72 %. In addition, in the case of Authentication ECC and Integrity SHA-3 algorithms, the total sum of probability of channel Collision is 0.465, and total average of PDR is 99.84%, thus the secure system with both authentication and integrity is better than implementation of only either of them (authentication or integrity).

4.3.4 The normal cognitive radio system (without security algorithm)

It is used to verify and to prove that the security system enhances the cognitive radio network with specific level of security in state of data integrity and authentication. It is simulated with OMNET++ without any level of security. Figure 4.21 shows the normal state and data transmitted among cognitive radio nodes and it is acknowledged with the proposed normal state.

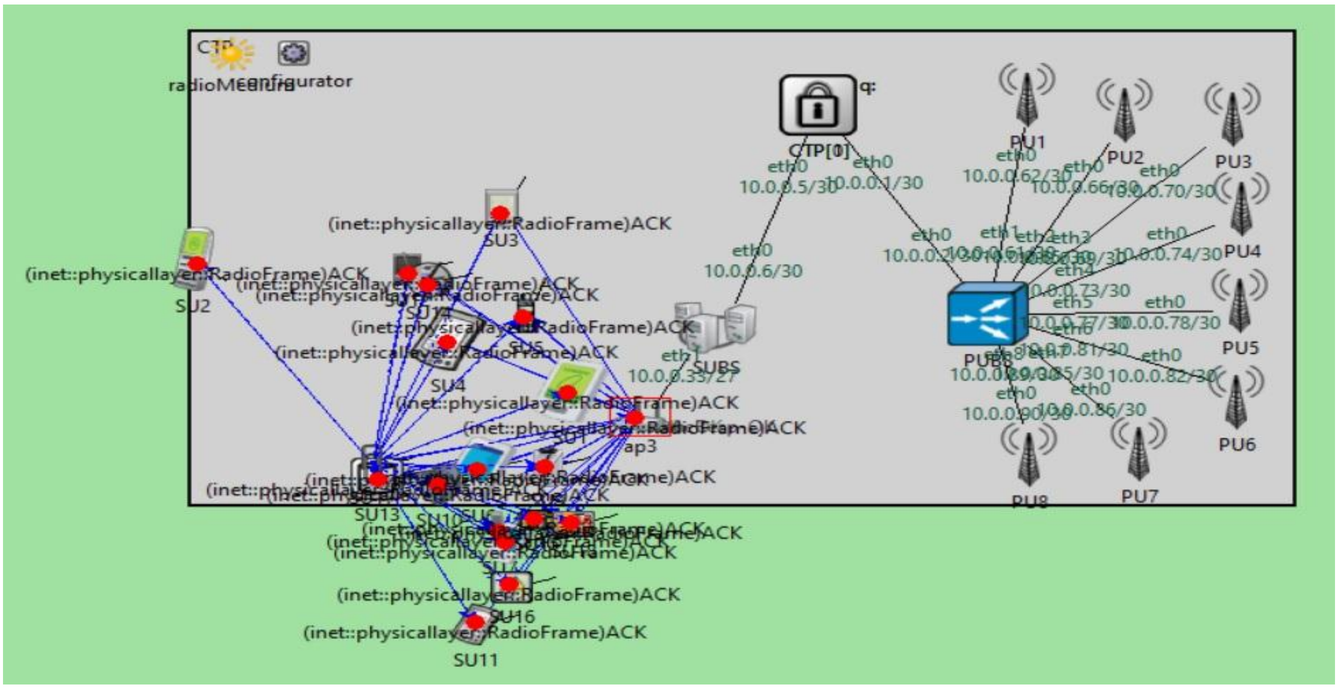


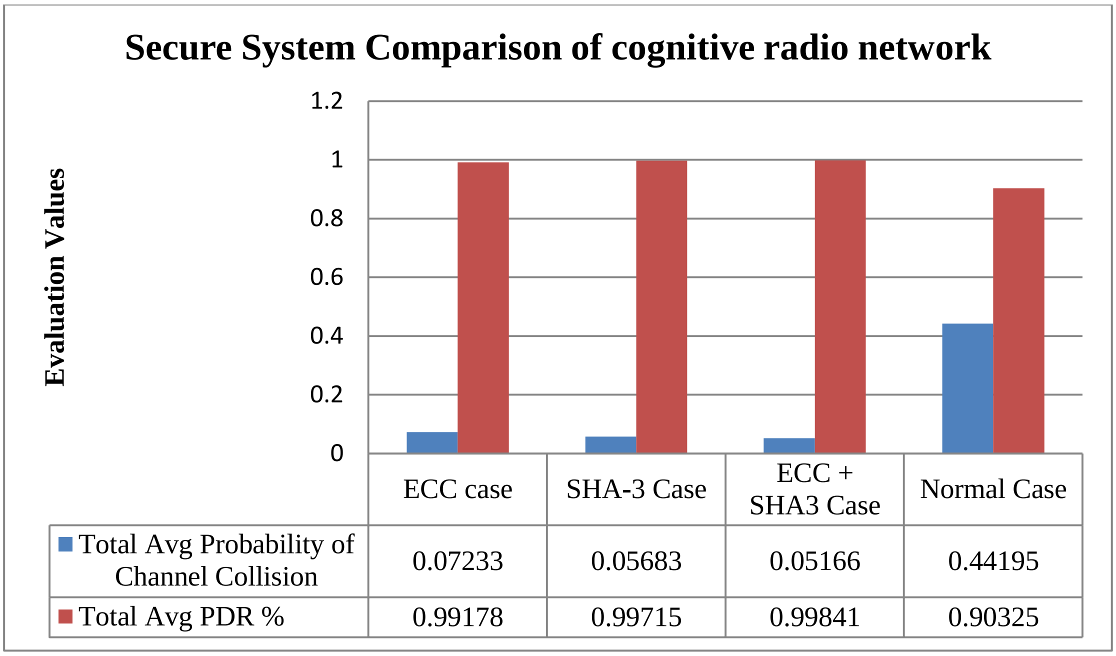
Figure 4.21 : Normal data transmitted and acknowledged.

Table 4.30 shows the evaluation state of the normal case of the proposed cognitive radio network. Probability of channel collision increases in both above mentioned cases of authentication and integrity due to the increasing number of nodes without authentication nodes and without ensuring that data modification affects the total successful arriving packets without errors to the destination secondary user; therefore, the network is overloaded usage with a huge amount of packets without acknowledgement and reliable traffic from authenticated users.

Table 4.30: The normal cognitive radio system (without security algorithm)

Data Type	**Network Elements**		**Payload Throughput / Bps**		**Probability of Channel Collision**	**PDR %**
	Send Nodes	**Received Nodes**	**Packets/sec Sent**	**Packets/sec Received**		
Text	CR 1	RC2	242.12	217.2	0.59	89.707 %
	CR 3	RC4	255.85	231.6	0.69	90.521 %
	CR 5	RC6	234.4	214.68	0.49	91.587 %
Image	CR 7	RC8	430950	393480	0.2899	91.305 %
	CR 9	RC10	385320	353400	0.3119	91.716 %
	CR 11	RC12	405320	352200	0.225	86.894 %
File	CR 13	RC 14	16286400	14872800	0.4784	91.320 %
	CR 15	RC 16	13216800	11846400	0.3676	89.631 %
	CR 17	CR 18	14052800	12681600	0.5348	90.242 %

The best result is the case of ECC and SHA-3 due to the channel is controlled and check point is created to make sure only authorized cognitive radio node is available in the transmission medium and increased number of data messaged arrived without errors .



	ECC case	SHA-3 Case	ECC + SHA3 Case	Normal Case
🟦 Total Avg Probability of Channel Collision	0.07233	0.05683	0.05166	0.44195
🟥 Total Avg PDR %	0.99178	0.99715	0.99841	0.90325

Figure 4.22 : Secure system comparison of the second system case study.

Chapter Five

Conclusions and Suggestions for Future Works

5.1Conclusions

This chapter explains the proposed system conclusions and the main suggestions for future works they can be summarized as :

1- The proposed CRNs architecture is based on the five communication layers for data transmission. Each layer responsibilities within the proposal security system is presented with C ++ programming language module inside OMNET++ simulation.

A- Security approach with Crypto system AES, RC5 Encryption Algorithms

B- Security approach with Cognitive Trusted Party (CTP) Model

2- The better performance of the 1st security system as total average throughput of sent packets of 4 SUs and 10 PUs is 4.7 Bps of 8 SUs and 20 PUs is 8.9 Bps, 16 SUs and 30 PUs is 7.2 Bps. Fuzzy Logic channel enhancement with 16 SUs and 30 PUs is 7.8125 Bps. Total average throughput of received packets with 4 SUs and 10 PUs is 4.6 Bps; 8 SUs and 20 PUs is 8.625 Bps, 16 SUs and 30 PUs is 7.075 Bps. Fuzzy Logic with 16 SUs and 30 PUs is 7.7125 Bps. Total average packet loss rate of 4 SUs and 10 PUs is 0.1 %; 8 SUs and 20 PUs is 0.275 %; 16 SUs and 30 PUs 0.125 %. Fuzzy Logic with 16 SUs and 30 PUs is 0.1 %. It shows the case of fuzzy logic for resource allocation is better than other cases due to the increasing number of idle channels provided by model to transmit secondary user data.

3- The better performance of the 2nd security system is total average probability of channel collision of ECC case is 0.0723, SHA-3 case is 0.0568, ECC with SHA3 case is 0.0516. Total average PDR of ECC case is 99.17 %, SHA-3 Case is 0.99.71 %, and integrated system of ECC with SHA3 Case is 99.84 %.

4- The results show the proposed security system succeeds in authenticating secondary users can associate and access to idle channel.

5- The second security system under consideration exhibits robust and impregnable defense mechanisms against various attacks pertaining to user authentication and data integrity. These include, but are not limited to session-specific random number leakage attacks, replay attacks, key compromise impersonation, and insider attacks. Furthermore, it exhibits the concept of mutual authorization and the implementation of perfect forward secrecy.

5.2 Suggestions for Future Research

There are numerous considerations can be realized for future expansion of present research through utilizing the following directions:

1- Improving technique for detecting Primary User Emulation (PUE) attacks in cognitive radio networks and further addressed the characteristics of sparsely populated cognitive radio networks and the mobility of the primary users.

2- Implementing machine learning approach dynamically indicate path for effective data transmission between network cognitive trusted party and base stations.

3- Secure dynamic channel estimation-aware for secure routing protocol at network layer in many application of wireless cognitive radio networks for instance smart Industrial automation IIoT applications.

4- Applying a Blockchains based smart contract in cognitive radio networks, which are based upon a permissioned blockchain that helps in making the transactions private among the participants. Further, the efficiency of this approach is improved by introducing a reputation parameter for the users. This measures the trustworthiness of a particular user based upon the accuracy of their recent sensing results.

5- Developing a lightweight secure cognitive radio-enabled wireless sensor networks by integrating both WSN and CRN technologies for improving channel utilization and network performance.

REFERENCES

[1] Salahdine, F., & Kaabouch, N. (2020). Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. *Physical Communication*, *39*, 101001.

[2] Ramkumar, J., & Vadivel, R. (2020). Bee inspired secured protocol for routing in cognitive radio ad hoc networks. *Indian J. Sci. Technol*, *13*(30), 3059-3069.

[3] Kumar, A., & Kumar, K. (2020). Multiple access schemes for cognitive radio networks: A survey. *Physical Communication*, *38*, 100953.

[4] Do-Dac, T., & Ho-Van, K. (2021). Energy harvesting cognitive radio networks: security analysis for Nakagami-m fading. *Wireless Networks*, *27*(3), 1561-1572.

[5] Uribe, J. D. J. R., Guillen, E. P., & Cardoso, L. S. (2022). A technical review of wireless security for the internet of things: Software defined radio perspective. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 4122-4134.

[6] Chithaluru, P., Al-Turjman, F., Stephan, T., Kumar, M., & Mostarda, L. (2021). Energy-efficient blockchain implementation for cognitive wireless communication networks (CWCNs). *Energy Reports*, *7*, 8277-8286.

[7] Malik, M., Dutta, M., & Granjal, J. (2019). A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. *IEEE Access*, *7*, 27443-27464.

[8] Baksi, A., Bhasin, S., Breier, J., Jap, D., & Saha, D. (2022). A survey on fault attacks on symmetric key cryptosystems. *ACM Computing Surveys*, *55*(4), 1-34.

[9] Usman, M., Amin, R., Aldabbas, H., & Alouffi, B. (2022). Lightweight challenge-response authentication in SDN-based UAVs using elliptic curve cryptography. *Electronics*, *11*(7), 1026.

REFERENCES

[10] Abood, Z. A., & Sadkhan, S. B. (2022, May). Security evaluation techniques of Cognitive Radio Network status and challenges. In *2022 5th International Conference on Engineering Technology and its Applications (IICETA)* (pp. 265-270). IEEE.

[11] Mapunya, S., & Velempini, M. (2018). Investigating spectrum sensing security threats in cognitive radio networks. In *Ad Hoc Networks: 9th International Conference, AdHocNets 2017, Niagara Falls, ON, Canada, September 28–29, 2017, Proceedings* (pp. 60-68). Springer International Publishing

[12] Develi, I. (2020). Spectrum sensing in cognitive radio networks: threshold optimization and analysis. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 1-19.

[13] Aksatha, D. S. D., & Pugazendi, R. (2020). A FUZZY LOGIC SYSTEM FOR IMPROVING THE PERFORMANCE OF QoS IN ENERGY EFFICIENCY USING COGNITIVE RADIO. *International Journal of Management (IJM)*, *11*(10).

[14] Chakraborty, A., Banerjee, J. S., & Chattopadhyay, A. (2020). Malicious node restricted quantized data fusion scheme for trustworthy spectrum sensing in cognitive radio networks. *Journal of mechanics of continua and mathematical sciences*, *15*(1), 39-56.

[15] Monisha, M., & Rajendran, V. (2022). SCAN-CogRSG: Secure channel allocation by dynamic cluster switching for cognitive radio enabled smart grid communications. *IETE Journal of Research*, *68*(4), 2826-2847.

[16] Ponnrajakumari, M., Devik, V., & BR, T. B. (2021). A NOVEL SECURE AND RELIABLE CLUSTERING PROTOCOL FOR COGNITIVE RADIO NETWORK USING FUZZY CLUSTERING AND MATHEMATICAL

FIBONACCI SERIES BASED GOLDEN RATIO OPTIMIZATION. *Dynamic Systems and Applications*, *30*(6), 1042-1061.

[17] Sasipriya, S., Bhuvaneswari, M., Kumar, P. M. V., & Karthikeyan, C. (2022). Efficient Resource Distribution in Cognitive Radio Network by Fuzzy-Based Cluster Against Attacks. In *IOT with Smart Systems: Proceedings of ICTIS 2021, Volume 2* (pp. 9-18). Singapore: Springer Nature Singapore.

[18] L. Nassef and R. Al-Hebshi, "Fuzzy based Reliable Cooperative Spectrum Sensing for Smart Grid Environment," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, 2020, doi: https://doi.org/10.14569/ijacsa.2020.0110822.

[19] VasanthaReddy, R. M., & Lingareddy, S. C. (2021). Detection and Prevention of Primary User Emulation Attack in Cognitive Radio Networks Using Secure Hash Algorithm. *International Journal of Intelligent Engineering & Systems*, *14*(2).

[20] Lafia, D., Sanni, M. L., Adetona, R. A., Akinyemi, B. O., & Aderounmu, G. A. (2021). Signal Processing-based Model for Primary User Emulation Attacks Detection in Cognitive Radio Networks. *Journal of computing and information technology*, *29*(2), 77-88.

[21] Ali, A., Abbas, L., Shafiq, M., Bashir, A. K., Afzal, M. K., Liaqat, H. B., Kwak, K. S. (2019). Hybrid fuzzy logic scheme for efficient channel utilization in cognitive radio networks. *IEEE Access*, *7*, 24463-24476.

[22] Jaganathan, R., & Vadivel, R. (2020). Intelligent fish swarm inspired protocol (IFSIP) for dynamic ideal routing in cognitive radio ad-hoc networks. *International Journal of Computing and Digital Systems*, *10*, 2-11.

[23] Robert, V. N. J., & Vidya, K. (2023). Genetic algorithm optimized fuzzy decision system for efficient data transmission with deafness avoidance in

multihop cognitive radio networks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(2), 959-972.

[24] Jain, P. P., Pawar, P. R., Patil, P., & Pradhan, D. (2019). Narrowband spectrum sensing in cognitive radio: Detection methodologies. *International Journal of Computer Sciences and Engineering*, *7*(11), 105-113.

[25] Liang, W., Di Wang, K., Shi, J., Li, L., & Karagiannidis, G. K. (2019). Distributed sequential coalition formation algorithm for spectrum allocation in underlay cognitive radio networks. *IEEE Access*, *7*, 56803-56816.

[26] Chitnavis, S., & Kwasinski, A. (2019, April). Cross layer routing in cognitive radio networks using deep reinforcement learning. In *2019 IEEE wireless communications and networking conference (WCNC)* (pp. 1-6). IEEE.

[27] 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.

[28] Bariah, L., Muhaidat, S., & Al-Dweik, A. (2019). Error performance of NOMA-based cognitive radio networks with partial relay selection and interference power constraints. *IEEE Transactions on Communications*, *68*(2), 765-777.

[29] Bala, I., Ahuja, K., & Nayyar, A. (2021). Hybrid spectrum access strategy for throughput enhancement of cognitive radio network. In *Micro-Electronics and Telecommunication Engineering: Proceedings of 4th ICMETE 2020* (pp. 105-122). Singapore: Springer Singapore.

[30] Sharmila, A., & Dananjayan, P. (2019, March). Spectrum sharing techniques in cognitive radio networks–A survey. In *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)* (pp. 1-4). IEEE.

REFERENCES

[31] Sharmila, A., & Dananjayan, P. (2019, March). Spectrum sharing techniques in cognitive radio networks–A survey. In *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)* (pp. 1-4). IEEE.

[32] Zhuang, Y., Li, X., Ji, H., Zhang, H., & Leung, V. C. (2020). Optimal resource allocation for RF-powered underlay cognitive radio networks with ambient backscatter communication. *IEEE Transactions on Vehicular Technology*, *69*(12), 15216-15228.

[33] Lameiro, C., Santamaria, I., Schreier, P. J., & Utschick, W. (2019). Maximally improper signaling in underlay MIMO cognitive radio networks. *IEEE Transactions on Signal Processing*, *67*(24), 6241-6255.

[34] Zhao, D., Qin, H., Song, B., Han, B., Du, X., & Guizani, M. (2020). A graph convolutional network-based deep reinforcement learning approach for resource allocation in a cognitive radio network. *sensors*, *20*(18), 5216.

[35] Liu, X., Sun, C., Yu, W., & Zhou, M. (2021). Reinforcement-Learning-based dynamic spectrum access for software-defined cognitive industrial internet of things. *IEEE Transactions on Industrial Informatics*, *18*(6), 4244-4253.

[36] Song, H., Liu, L., Ashdown, J., & Yi, Y. (2021). A deep reinforcement learning framework for spectrum management in dynamic spectrum access. *IEEE Internet of Things Journal*, *8*(14), 11208-11218.

[37] 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.

[38] Benedetto, F., Mastroeni, L., & Quaresima, G. (2021, July). Auction-based theory for dynamic spectrum access: A review. In *2021 44th International*

Conference on Telecommunications and Signal Processing (TSP) (pp. 146-151). IEEE.

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

[40] Aslam, M. M., Du, L., Zhang, X., Chen, Y., Ahmed, Z., & Qureshi, B. (2021). Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges. *Wireless Communications and Mobile Computing*, *2021*, 1-18.

[41] Mohammed, D. A., & Sadkhan, S. B. (2021, April). Cooperative Cognitive Radio Sensing-Optimization: status, challenges and future Trends. In *2021 1st Babylon International Conference on Information Technology and Science (BICITS)* (pp. 164-169). IEEE.

[42] Sadkhan, S. B., & Jabbar, D. (2021, June). The Security Challenges with Cognitive Radio Environments for VANETS. In *2021 International Conference on Communication & Information Technology (ICICT)* (pp. 167-173). IEEE.

[43] Benmammar, B. (2021). Internet of things and cognitive radio: Motivations and challenges. *International Journal of Organizational and Collective Intelligence (IJOCI)*, *11*(1), 39-52.

[44] Nasser, A., Al Haj Hassan, H., Abou Chaaya, J., Mansour, A., & Yao, K. C. (2021). Spectrum sensing for cognitive radio: Recent advances and future challenge. *Sensors*, *21*(7), 2408.

[45] Nallarasan, V., & Kottilingam, K. (2021, January). Spectrum management analysis for cognitive radio IoT. In *2021 international conference on computer communication and informatics (ICCCI)* (pp. 1-5). IEEE.

REFERENCES

[46] Sivagurunathan, P. T., Ramakrishnan, P., & Sathishkumar, N. (2021). Recent paradigms for efficient spectrum sensing in cognitive radio networks: Issues and challenges. In *Journal of Physics: Conference Series* (Vol. 1717, No. 1, p. 012057). IOP Publishing.

[47] Hassan, M., Singh, M., & Hamid, K. (2021, March). Overview of cognitive radio networks. In *Journal of Physics: Conference Series* (Vol. 1831, No. 1, p. 012013). IOP Publishing.

[48] Ramaiah, V. S., Singh, B., Raju, A. R., Reddy, G. N., Saikumar, K., & Ratnayake, D. (2021, March). Teaching and Learning based 5G cognitive radio application for future application. In *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (pp. 31-36). IEEE.

[49] Jasim, D. K., & Sadkhan, S. B. (2021, September). The eavesdropping attack on security tradeoff for cognitive radio networks. In *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)* (pp. 223-229). IEEE.

[50] Ibrahim, N. K., Sali, A., Karim, H. A., Ramli, A. F., Ibrahim, N. S., & Grace, D. (2022). Multiple description coding for enhancing outage and video performance over relay-assisted cognitive radio networks. *IEEE Access*, *10*, 11750-11762.

[51] Helmy, M., Hassan, M. S., & Ismail, M. H. (2022). Spectrum allocation techniques for cognitive radio networks. *IEEE Access*, *10*, 28180-28193.

[52] Iqbal, J., Adnan, M., Khan, Y., AlSalman, H., Hussain, S., Ullah, S. S., ... & Gumaei, A. (2022). Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis. *Journal of Healthcare Engineering*, *2022*, 1-19.

REFERENCES

[53] Abdel-Razeq, S., Salameh, H. B., & Al-Obiedollah, H. (2022, December). Integrating Cognitive Radio in NOMA-based B5G Networks: Architecture and Research Challenges. In *2022 Seventh International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 1-6). IEEE.

[54] Tan, X., Zhou, L., Wang, H., Sun, Y., Zhao, H., Seet, B. C., ... & Leung, V. C. (2022). Cooperative Multi-Agent Reinforcement-Learning-Based Distributed Dynamic Spectrum Access in Cognitive Radio Networks. *IEEE Internet of Things Journal*, *9*(19), 19477-19488.

[55] Kafetzis, D., Vassilaras, S., Vardoulias, G., & Koutsopoulos, I. (2022). Software-defined networking meets software-defined radio in mobile ad hoc networks: State of the art and future directions. *IEEE Access*, *10,* 9989-10014.

[56] Dalloz, N., Le, V. D., Hebert, M., Eles, B., Flores Figueroa, M. A., Hubert, C., ... & Destouches, N. (2022). Anti-Counterfeiting White Light Printed Image Multiplexing by Fast Nanosecond Laser Processing. *Advanced Materials*, *34*(2), 2104054.

[57] Velastegui, N., Pavon, E., Jacome, H., Torres, F., & Pico, M. (2022). Technological advances in military communications systems and equipment. *Revista Minerva: Multidisciplinaria de Investigación Científica*, *3*(8), 61-73.

[58] LaCasse, P. M., Champagne, L. E., & Escamilla, J. M. (2022). Simulation analysis of applicant scheduling and processing alternatives at a military entrance processing station. *The Journal of Defense Modeling and Simulation*, 15485129221134536.

[59] Rohokale, V. M., & Prasad, R. (2022). Cyber Security-The Essence of CONASENSE. In *Security within CONASENSE Paragon* (pp. 1-10). River Publishers.

REFERENCES

[60] Jasim, D. K., & Sadkhan, S. B. (2021, April). Cognitive radio network: Security and reliability trade-off-status, challenges, and future trend. In *2021 1st Babylon International Conference on Information Technology and Science (BICITS)* (pp. 149-153). IEEE.

[61] Yan, Z., Kong, H., Wang, W., Liu, H. L., & Shen, X. (2021). Reliability benefit of location-based relay selection for cognitive relay networks. *IEEE Internet of Things Journal*, *9*(3), 2319-2329.

[62] Wu, X., Ma, J., Xing, Z., Gu, C., Xue, X., & Zeng, X. (2021). Secure and energy efficient transmission for IRS-assisted cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking*, *8*(1), 170-185.

[63] Wang, D., Zhou, F., Lin, W., Ding, Z., & Al-Dhahir, N. (2022). Cooperative hybrid nonorthogonal multiple access-based mobile-edge computing in cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking*, *8*(2), 1104-1117.

[64] Abood, Z. A., & Sadkhan, S. B. (2022, May). Security evaluation techniques of Cognitive Radio Network status and challenges. In *2022 5th International Conference on Engineering Technology and its Applications (IICETA)* (pp. 265-270). IEEE.

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

[66] Banumathi, J., Sangeetha, S. K. B., & Dhaya, R. (2022). Robust Cooperative Spectrum Sensing Techniques for a Practical Framework Employing Cognitive Radios in 5G Networks. *Artificial Intelligent Techniques for Wireless Communication and Networking*, 121-138.

[67] Gajewski, P., Łopatka, J., & Łubkowski, P. (2022). Performance analysis of public safety cognitive radio MANET for diversified traffic. *Sensors*, *22*(5), 1927.

REFERENCES

[68] Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. International Journal of Communication Networks and Information Security, 12(2), 256-272.

[69] Hossen, M. S., Islam, M. A., Khatun, T., Hossain, S., & Rahman, M. M. (2020, September). A new approach to hiding data in the images using steganography techniques based on AES and RC5 algorithm cryptosystem. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 676-681). IEEE.

[70] Afghah, F., Cambou, B., Abedini, M., & Zeadally, S. (2018). A reram physically unclonable function (reram puf)-based approach to enhance authentication security in software defined wireless networks. *International Journal of Wireless Information Networks*, *25*, 117-129.

[71] Yue, X., Liu, Y., Wang, J., Song, H., & Cao, H. (2018). Software defined radio and wireless acoustic networking for amateur drone surveillance. *IEEE Communications Magazine*, *56*(4), 90-97.

[72] Hu, X., Cheng, J., Zhou, M., Hu, B., Jiang, X., Guo, Y., ... & Wang, F. (2018). Emotion-aware cognitive system in multi-channel cognitive radio ad hoc networks. *IEEE Communications Magazine*, *56*(4), 180-187.

[73] Darney, D. P. E., & Jacob, D. I. J. (2019). Performance enhancements of cognitive radio networks using the improved fuzzy logic. *Journal of Soft Computing Paradigm*, *1*(2), 57-68.

[74] Mahmood, K., Chaudhry, S. A., Naqvi, H., Kumari, S., Li, X., & Sangaiah, A. K. (2018). An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, *81*, 557-565.

REFERENCES

[75] Núñez Segura, G. A., Margi, C. B., & Chorti, A. (2019). Understanding the performance of software defined wireless sensor networks under denial of service attack. *Open Journal of Internet Of Things (OJIOT), 5*(1), 58-68.

[76] Fu, Y., & He, Z. (2019). Bayesian-inference-based sliding window trust model against probabilistic SSDF attack in cognitive radio networks. *IEEE Systems Journal*, *14*(2), 1764-1775.

[77] Zhao, F., Li, S., & Feng, J. (2019). Securing cooperative spectrum sensing against DC-SSDF attack using trust fluctuation clustering analysis in cognitive radio networks. *Wireless Communications and Mobile Computing*, *2019*.

[78] Sohu, I. A., Rahimoon, A. A., Junejo, A. A., Sohu, A. A., & Junejo, S. H. (2019, January). Analogous study of security threats in cognitive radio. In *2019 2nd International conference on computing, mathematics and engineering technologies (iCoMET)* (pp. 1-4). IEEE.

[79] Berges, P. M. (2019). *Exploring the vulnerabilities of traffic collision avoidance systems (TCAS) through software defined radio (SDR) exploitation* (Doctoral dissertation, Virginia Tech).

[80] Le Roy, F., Roland, C., Le Jeune, D., & Diguet, J. P. (2019, August). Risk assessment of SDR-based attacks with UAVs. In *2019 16th International Symposium on Wireless Communication Systems (ISWCS)* (pp. 222-226). IEEE.

[81] Nguyen, V. L., Lin, P. C., & Hwang, R. H. (2019). Energy depletion attacks in low power wireless networks. *IEEE Access*, *7*, 51915-51932.

[82] Alcala'Garrido, H. A., Rivero-Angeles, M. E., & Anaya, E. A. (2019). Primary user emulation in cognitive radio-enabled WSNs for structural health monitoring: modeling and attack detection. *Journal of Sensors*, *2019*.

REFERENCES

[83] Arun, S., & Umamaheswari, G. (2020). An adaptive learning-based attack detection technique for mitigating primary user emulation in cognitive radio networks. *Circuits, Systems, and Signal Processing*, *39*, 1071-1088.

[84] Murmu, M. K., & Singh, A. K. (2020). Security issues in cognitive radio ad hoc networks. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 247-264.

[85] Kadhim, A. A., & Sadkhan, S. B. (2020, July). Cognitive Radio Performance Enhancement Based on Frequency Hopping System. In *2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA* (pp. 109-114). IEEE.

[86] Ganesh Babu, R., Obaidat, M. S., Amudha, V., Manoharan, R., & Sitharthan, R. (2020). Comparative analysis of distributive linear and non-linear optimised spectrum sensing clustering techniques in cognitive radio network systems'. *IET Networks*, *20*(1), 1-11.

الخلاصة

تعد شبكة الراديو الإدراكية (CRN) تقنية مهمة نظرًا لقدرتها على حل المشكلة بين العرض المحدود للطيف والطلب على الطيف من التطبيقات والخدمات اللاسلكية المتنامية. ومع ذلك، نظرًا لطبيعة هذه الشبكات، تتعرض شبكات CRN لأنواع مختلفة من التهديدات والهجمات من مستخدمين ضارين مختلفين، مما قد يؤثر على توفر الشبكة وأدائها. يعتمد النظام المقترح على تعزيز أمن الشبكة الراديوية المعرفية لتطبيق البيئة، وذلك باستخدام طريقتين آمنتين: الطريقة الأولى هي خوارزميات التشفير (AES، RC-5) لتشفير البيانات في OMNET++ وتخصيص القناة باستخدام طريقة Fuzzy Logic، والطريقة الثانية هي نهج الطرف المعرفي الموثوق به (CTP) لتوفير التكامل مع خوارزمية التجزئة الآمنة (SHA-3) والمصادقة باستخدام تشفير (ECC).

يتم قياس أفضل أداء لنظام الأمان الأول من خلال إجمالي متوسط إنتاجية الحزم المرسلة المكونة من 4 مستخدم ثانوي SU و10 مستخدم رئيسي PU وهو 4.7 بت في الثانية و8 وحدات SU؛ من 20 وحدة PU هي 8.9 نقطة أساس؛ 16 وحدة SU و30 وحدة PU تبلغ 7.2 نقطة في الثانية. يبلغ تحسين Fuzzy Logic باستخدام 16 مستخدم ثانوي SU و30 مستخدم رئيسي هي PU 7.8125 بت في الثانية.

يتم حساب أفضل أداء لنظام الأمان الثاني بمتوسط إجمالي لاحتمال تصادم القنوات لحالة ECC بقيمة 0.0723؛ حالة SHA-3 كـ 0.0568؛ وECC مع حالة SHA3 كـ 0.0516. إجمالي متوسط نسبة تسليم الحزم (PDR) لحالة ECC هو 99.17%؛ تبلغ نسبة حالة SHA-3 0.99.71%، والنظام المتكامل لـ ECC مع حالة SHA3 هو 99.84%. أفضل النتائج بدون أمان مقارنة بالأعمال ذات الصلة حيث أن تخصيص موارد Fuzzy Logic لقيمة PDR هي 98.71 % ومعدل إسقاط الحزم هو 10%.

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
تكنولوجيا المعلومات
قسم شبكات المعلومات

التخصيص الفعال للمستخدم الأساسي في التطبيق البيئي الآمن للراديو الإدراكي

رسالة مقدمة

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

من قبل الطالب

زمزم علي عبود نوري

باشراف

أ.د ستار بدر سدخان

هـ ١٤٤٥ م ٢٠٢٣