INTRUSION DETECTION AND RESPONSE MODEL TO ENHANCE SECURITY IN COGNITIVE RADIO NETWORKS

By

OHAERI, IFEOMA UGOCHI
(STUDENT NUMBER: 23989688)

DISSERTATION SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE (MSc.) IN COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE
SCHOOL OF MATHEMATICAL AND PHYSICAL SCIENCES
FACULTY OF AGRICULTURE, SCIENCE AND TECHNOLOGY
NORTH-WEST UNIVERSITY, MAFIKENG CAMPUS

SUPERVISOR: PROFESSOR O. O. EKABUA

OCTOBER, 2012

Declaration

I declare that this research project on **Intrusion Detection and Response Model to Enhance Security in Cognitive Radio Networks** is my work, and has never been presented for the award of any degree in any university. All sources of information used have been duly acknowledged both in text and in the references.

Signature_____ Date _____

Ohaeri, Ifeoma Ugochi

Approval

Signature_____

Supervisor: **Prof. O. O. Ekabua**
Department of Computer Science
Faculty of Agriculture Science and Technology
North-West University- Mafikeng Campus
South Africa

Dedication

This research dissertation is specially dedicated to:

My beloved Mother - **Hon. Chief Mrs Theresa Ohaeri**

and

My dearest Husband - **Mr Emmanuel O. Onwughara**

with whose great love, advice, patience and sacrifices have brought me to this level of academic attainment.

Acknowledgements

Firstly, I wish to express my profound gratitude to God Almighty, the pillar of my life for his love and kindness, and for enabling me to successfully complete this research project and the programme against of all odds.

I am absolutely indebted and grateful to Prof. O. O. Ekabua, my supervisor and Head of Department of Computer Science at North West University Mafikeng Campus. His motivation, inspiration, advice, support, useful discussions, useful criticisms and rare patience while carrying out this research project cannot be quantified and over emphasized. The Almighty God will reward you immeasurably.

I also appreciate my friends and research colleagues, Dladlu Nosipho, Thuso Muoemi, Micheal Mbougni, Peter Bigala, Eric-Nwoye, Nnenna Christine and most especially Mr Bassey Isong, for their help and support during the course of this research project.

My special appreciation goes to my late Dad, late Chief Mojekwu Ohaeri for his great love, sacrifices and denials that has sustained my dreams to this moment. His high aspirations have kept my vision from fading. I also specially appreciate my Mum, Hon. Chief Mrs Teresa Ohaeri. She has ever been my fountain of inspiration, source of motivation, encouragement and true love; she has never ceased to believe in me. Her immeasurable support kept me going through difficult times. Mum, you remain my hero.

Lastly, I most especially acknowledge my husband and my love Mr Emmanuel O. Onwughara, for his undying love, understanding, tolerance, encouragement, total support in all ramifications, and above all for believing in me. May the Almighty God bless and preserve your life.

Abstract

With the rapid proliferation of new technologies and services in the wireless domain, spectrum scarcity has become a major concern. Cognitive radios (CRs) arise as a promising solution to the scarcity of spectrum. A basic operation of the CRs is spectrum sensing. Whenever a primary signal is detected, CRs have to vacate the specific spectrum band. Malicious users can mimic incumbent transmitters so as to enforce CRs to vacate the specific band. Cognitive radio networks (CRNs) are expected to bring an evolution to the spectrum scarcity problem through intelligent use of the fallow spectrum bands. However, as CRNs are wireless in nature, they face all common security threats found in the traditional wireless networks. Common security combating measures for wireless environments consist of authorization, authentication, and access control. But CRNs face new security threats and challenges that have arisen due to their unique cognitive (self-configuration, self-healing, self-optimization, and self-protection) characteristics. Because of these new security threats, the use of traditional security combating measures would be inadequate to address the challenges. Consequently, this research work proposes an Intrusion Detection and Response Model (IDRM) to enhance security in cognitive radio networks. Intrusion detection monitors all the activities in order to detect the intrusion. It searches for security violation incidents, recognizes unauthorized accesses, and identifies information leakages. Unfortunately, system administrators neither can keep up with the pace that an intrusion detection system is delivering responses or alerts, nor can they react within adequate time limits. Therefore, an automatic response system has to take over this task by reacting without human intervention within the cognitive radio network.

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

ACE	Access Control Enforcement
BTS	Base Transceiver Stations
CCC	Cognitive Control Channel
CR	Cognitive Radio
CRN	Cognitive Radio Network
CRNIS	Cognitive Radio Network Information System
CSCC	Common Spectrum Coordination Channel
DoS	Denial of Service
DSA	Dynamic Spectrum Access
DSS	Distributed Spectrum Sensing
DSSS	Direct Sequence Spread Spectrum
FCC	Federal Communication Commission
GSM	Global System Mobile Communication
HIDS	Host-based Intrusion Detection System
ID	Identity
IDP	Intrusion Detection Prevention
IDS	Identity-based Security
IDS	Intrusion Detection System
IDRM	Intrusion Detection and Response Model
IDES	Intrusion Detection Expert System
IEEE	Institute of Electrical Electronics Engineering
ISS	Internet Security System
IMEI	International Mobile Equipment Identity
ITU	International Telecommunication Union
LAN	Local Area Network
LEAP	Light Extensible Authentication Protocol
MAC	Medium Access Control
MIDAS	Multics Intrusion Detection Alert System
NCSC	National Computer Security Centres

NIDSs	Network-based Intrusion Detection System
NSA	Network Security Administrator
NSAs	Network Security Administrators
PCs	Personal Computers
PDAs	Personal Digital Assistance
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PEAP	Protected Extensible Authentication Protocol
QoA	Quality of Assurance
QoS	Quality of Service
RQ	Research Questions
RF	Radio Frequency
RFID	Radio Frequency Identity
SDR	Software Defined Radio
SIM	Subscriber Identity Module
SGMP	Simple Gate Management Protocol
SNMP	Simple Network Management Protocol
SPEA	Security Policy Enforcement Agent
SPDA	Security Policy Decision Agent
SPRA	Security Policy Retrieval Agent
TDMA	Time Division Multiple Access
TCP/IP	Transport Control Protocol/ Internet Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WEP	Wired Extensible Protocol
WPA	Wi-Fi Protected Access
Wi Max	World Wide Interoperability for Microwave Access
Wi-Fi AP	Wireless Fidelity Authentication Protocol
WRANs	Wireless Regional Area Networks

CHAPTER ONE
INTRODUCTION AND BACKGROUND

1.1 Chapter Overview

Cognitive Radio is a dynamic and intelligent wireless communication system that learns and understands and adapts to its physical environment –the outside world. It builds the methodology of understanding that is used to learn from the environment and invariably adapts its various internal states to any incoming Radio Frequency (RF) while conforming to certain policies and regulations. It does this by making changes in real time in some operating parameters such as: transmit power, modulation strategy and carrier-frequency, having in mind a highly reliable communication wherever and whenever and also an efficient utilization of the spectrum as its two primary objectives [1]. This means that communication between multiple users in cognitive radio network is achieved in a self-organized manner, to control the communication channels by allocating the available resources properly and to build an environment of self-configuration, self-awareness, adaptation, and self-optimization [2].

The need to integrate several wireless systems and networks and use each of them appropriately based on the communication environments and application requirements, reconfigurable communication and networking among other wireless technology that support Internet access and other stream services gave rise to the vision of Cognitive Radio as pioneered by J. Mitola III, from software defined radio (SDR). Cognitive Radio was considered originally to improve the utilization of the spectrum and was commissioned by the federal communication commission (FCC). Apparently, cognitive radio is a link-level technology primarily designed for dynamic access of radio spectrum to enable physical layer radio transmission as a kind of configurable wireless communication technology. Therefore, cognitive radio does not only provide spectrum advantages but also networking above link-layer to support the vision of integrated re-configurable systems and networking [3].

Moreover, once a cognitive radio network transporting packet on top of cognitive radio links discovers the opportunities to use the spectrum holes for communications, it is unavoidable to successfully facilitate and enhance useful application and services in other to maximize the opportunity. For example, if a cognitive radio terminal that has cognitive radio capabilities senses the communication environments such as spectrum holes, geographic location, available services and available wire and wireless communication systems or networks, it analyses it and gets information from the environment using the user preferences. It also demands to reconfigure itself by adjusting the system parameter while conforming to proper rules and regulations. In application, if a cognitive radio mobile terminal senses that there are Wi-Fi and GSM devices or systems available nearby and spectrum holes exist in the frequency band of the digital TV, it can decide to download files from the Wi-Fi AP, it can make phone calls through the GSM system and communicate with other cognitive radio devices (users) via the system holes. Apparently, cognitive radio terminals can also negotiate with other spectrum or network users to facilitate more efficient and effective spectrum and network utilization. This negotiation can be enabled by the support of network or infrastructure frameworks or in an ad hoc manner. However, the advantages of this new technology can be overridden by its security threats [4].

There are many factors that make security in cognitive radio networks a huge challenge which affects the management of data and information. Some of these factors include: control of access or denial of access, user groups with a large and dynamic resource pool, devices and resources having no authentication and authorization requirements, computations spanning over multiple domains, users having different privileges in different domains [5]. The distributed and wireless nature makes cognitive radio networks experience huge security challenges. These challenges make the network vulnerable to various malicious attacks. Hence an intrusion detection and response model becomes a suitable security infrastructure to enhance security and improve quality of service in CRN [6].

One of the means to provide a secured computational environment is rapid detection and response to network threats and attacks. In any ideal network environment, systems

should not be vulnerable to denial of service attacks, because access control mechanisms are capable of preventing all unauthorized users and intruders from having access to the network and intrusion detection would be irrelevant. However, networked systems have vulnerabilities and access control has imperfections, hence an intrusion detection and response model provides an improvement to other security mechanisms to enhance security and quality of service (QoS) in cognitive radio networks. [5].

Intrusion Detection and Response Model (IDRM) enhances security in cognitive radio networks by providing an enabling environment for rapid detection of intrusions for quality of service (QoS) and efficient resource allocation. The fundamental aims of security in cognitive radio-based wireless networks are secured communication through an effective access control technique and efficient usage of spectrum resources [7]. In the process of establishing these fundamentals, an Intrusion detection and response model is a necessity and an adequate security mechanism to be considered [8]. However, emphasis is made on security requirements such as authentication, authorization and firewall access control mechanisms that provide the first line of defense in cognitive radio networks [9].

IDRM security mechanism monitors an entire network to detect intrusions and intruders such as unexpected, unauthorized and unwanted users or programs disrupting network operations. It is capable of initiating a quick response once a malicious act or an unauthorized activity is taking place or has taken place within and outside the CR networked systems. However, when it is in an integral part of the CRN system and it is used in connection with other security measures such as authentication, authorization and firewall access control mechanisms, it provides adequate security standard for an effective dynamic management of data and information in other to provide an efficient quality of service [10]

The utmost intention of intruders is to disrupt communication flow within the network. They can utilize intrusion mechanisms and attack models to gain advantages and break down the entire network service completely. Consequently, security has become significant for effective and secured communication, interoperability, integration of resources and services across multiple users and network layers in CRN. Therefore, it is quite imperative to consider an intrusion detection and response model as an effective

and adequate security mechanism to provide secured communication and quality of service in cognitive radio network. [11].

1.2 Background Information

The growing need to standardize the knowledge, information and data structures related to the spectrum environment in order to enable mechanism and automated methods for spectrum access has led to the innovation of cognitive radio (CR). Cognitive radios are a new idea that was ushered in by the wireless medium as the beginning of a new modality in wireless networks. Cognitive radios are radios that gain awareness of their environment and surroundings and are capable of adapting their behavior accordingly. They possess enormous potential and abilities to increase the effectiveness and efficiency of wireless spectrum usage and develop devices and systems that are able to interact with other systems and users. A cognitive radio can discover an unused frequency band and utilize it for transmission, and later move over to another unused band when the current band is needed by a primary user. Apparently, cognitive radios need to share information between the physical layer and MAC layer of similar devices in compatible connection communicating together over a network, as against a conventional radio where the frequency band of a cognitive radio operates at a given time, depends largely on the channel occupancy measured at the physical layer, and transmitted to the MAC layer via an appropriate interface which requires a cross layer design [12, 13].

The radio spectrum is a scarce natural resource that gives network access to wireless devices. The increase in wireless technology and use of mobile devices has resulted in unavailability and overcrowding of the spectrum band. Intelligent cognitive radio devices sense, and discover "spectrum holes" (vacant or unused areas) that can be used for communications, whereas, hardware-based wireless and conventional hardware devices have the ability to only access specific area of the radio spectrum.

The spectrum utilization scheme is referred to as distributed spectrum sensing and sharing (DSS). Data and information management in cognitive radio network operates in a distributed form. Spectrum resources, which are limitless natural resources, are shared

by both primary and secondary users. DSS enables the use of the vacant spectrum bands without any interference to the primary users [11].

The dynamic spectrum allocates and distributes the free channels (vacant or unused areas) for the cognitive radio nodes that are demanding or striving for it [12]. However, CRN is capable of independently changing its physical layer behavior and present environment at any given time [13]. It is able to perform the adaptation strategy which is totally based on cognitive spectrum. Having these capabilities, when the spectrum environment alters within the cognitive radio users, it is able to sense these changes and immediately make adjustments. The physical layer settings like transmission power, channel detection and selection changes automatically and independently meet the constraints and quality of assurance (QoA) requirements of other spectrum users [6].

In the design of networks and systems, security should be considered from early phases. While this approach to security is important for consistent and efficient security decisions, it becomes critical in case of CRN systems. Hence, the cognitive radio network management system should be able to provide a security scheme, mechanism or infrastructure that will establish secured communications, and record the operations processed by the network users to identify intrusions and malicious activities in order to provide a secured communication environment and quality of service [14]. However, as CRNs are wireless in nature, they face all common security threats found in the traditional wireless networks as well as new security threats which entail majorly illegal information injection and forging of information transmission, denial of service attacks, license user emulation and others. These new security threats and challenges have arisen due to their unique cognitive (self-configuration, self-healing, self-optimization, and self-protection) characteristics. Attackers can maliciously falsify local spectrum sensing data to confuse the receiver and launch attacks which can prompt the receiver to make wrong spectrum accessing decisions [4]. Therefore, security that is built into the system should be inserted from metric. Usually, information technology and network security is majorly analyzed on the basics of confidentiality, integrity and availability. A secure computer network is a trusted and reliable system that functions appropriately [15]. In the 1980s, computer systems had been equipped already with an audit capability. The operating

systems is capable of collecting system-wide attributes and use them for audit trail but, the analysis being done by humans became very tedious as the use of wireless technology, collected events and activities increased.

Moreover, due to the new security threats and challenges introduced by the unique characteristics of cognitive radio networks, the use of traditional security combating measures such as authentication, authorization and firewalls which constitute the first line of defense would be inadequate to address the challenges. Therefore, an automated method of collecting and analyzing data to produce vital information to check network intrusions becomes very necessary. The birth of this automated mechanism or tool makes an Intrusion Detection and Response Model (IDRM) become very necessary for CRNs [16].

Consequently, this research project develops an Intrusion Detection and Response Model (IDRM) to enhance security in cognitive radio networks. Intrusion detection monitors all the activities in order to detect the intrusion. It searches for security violation incidents, recognizes unauthorized accesses, and identifies information leakages. Unfortunately, system administrators neither can keep up with the pace that an intrusion detection system is delivering responses or alerts, nor can they react within adequate time limits. Therefore, an automatic response system has to take over this task by reacting without human intervention within the cognitive radio networks.

The IDRM in practice monitors network activities to identify various attacks, threats or violations of security policy and generates an automatic response to combat the incident using a specified response technique [17]. This security mechanism is capable of examining packet traffic to discover its source and destination IP addresses together with source and destination ports. It identify network sessions and examining dialogs between the systems for multi-packet activity, examine and responding to entire conversations between hosts, and using knowledge of protocols and network sessions to analyze traffic to discover malicious activities. This activity entails the investigation of different protocol layers such as the physical layer, link layer, network layer transport layer and application layer to enable a good understanding and response to attacks and enhance security in cognitive radio networks [16]. It is expected of this monitoring system to not

only identify those possible security violations but also to stop any attempt of intrusion [18].

However, this system can also be used for other purposes such as identify problems with security policies, documenting existing threats, and stopping individuals from violating security policies. Usually, the intrusion detection systems (IDS) can detect intrusions by looking for specific signatures of common threats- the same way antivirus software specifically detects and protects against malware - some detect intrusions by comparing traffic patterns against a baseline and searching for anomalies. However, the IDRM developed in this research project not only monitors network traffic and examines networks patterns to detect intrusions but also performs an action or actions in response to a detected threat with the aim of providing an enabling environment for an effective dynamic management of data and information for efficient quality of service [19, 20].

1.3 Statement of Problem

Security, like any other system in the world, forms the vital aspect of cognitive radio networks due to its increasing nature of malicious activity and the need to ensure QoS. Mechanisms to protect cognitive radio networks and their resources against the array of threats militating per second must be put in place. Security should be embedded in the network design and configured at all borders to achieve reasonable security level [21].

Information Systems and Networks are subject to electronic attacks. Attempts to breach information security are rising every day, along with the availability of the Vulnerability Assessment tools that are widely available on the Internet, for free, as well as for a commercial use. Tools such as SubSeven, BackOrifce, Nmap, L0ftCrack, can all be used to scan, identify, probe, and penetrate your systems. Although there are firewalls in place to prevent unauthorized access to the CR networks, these firewalls are inadequate, less structured not as sophisticated as those used by experienced hackers. But are the firewalls enough in the midst of these sophisticated tools and experienced hackers?

Usually, firewalls are designed with holes that leave things through to the network which enables us to access the internet, send and receive e-mails, and attackers have the skill

and tools to bypass and cheat firewalls. The IDRM developed for CRNs does not sideline the first line or level of defense in information system and network security such as; authentication, authorization, firewall and other access control measures. These measures alone cannot guarantee a secured communication. Therefore, providing a secured channel of communication where all security measures put in place have been bypassed would require an intrusion detection and automated response model to identify such sophisticated network intrusions and automatically generate appropriate responses to combat such attacks [12].

The fundamental aim of security in cognitive radio-based wireless networks is secured communication through an effective access control technique and efficient usage of spectrum resources. In order to achieve this aim, an adequate security measure should be considered [8, 10]. However, in distributed wireless networks like CRNs, firewalls do not provide the reliable secured environment required because they are not capable of generating automated responses whenever intrusions or malicious activity is suspected or detected. Hence an intrusion detection and automated response model is most recommended to enhance security in CRNs [16]. Consequently, the IDRM becomes an integral part of CR networks to provide a secured communication and an enabling environment for efficient resource allocation, effective spectrum usage and access control [5].

1.4 Research Questions

In consideration of the above stated problem, this research project is addressing the following research questions (RQs).

How can an intrusion detection and response model:

RQ1: Identify the CRN users and ensure that intruders (malicious users) do not get access to the services (data and information) provided in the CR network?

RQ2: Detect intruders, intrusions (attacks) and other security violations common to CR networks?

RQ3: Enhance security and quality of service in cognitive radio networks?

1.5 Research Goal and Objectives

The main goal and objectives of this research are as follows:

1.5.1 Research Goal

The main goal of this research is to develop an intrusion detection and response model to enhance security in cognitive radio networks.

1.5.2 Research Objectives

In order to achieve the main goal of this research, the research had four objectives:

(i) To analyze current or existing endeavors on security in cognitive radio networks.

(ii) To investigate the vulnerabilities and attacks associated with cognitive radio networks.

(iii) To define the various security requirements for cognitive radio networks based on an Intrusion Detection and Response Model.

(iv) To develop and implement an IDRM for CR networks based on the requirements in objective (iii).

1.6 Research Methodology

The methodology used in this research consists of three steps: literature review, response model design, and prototype implementation as a proof of concept. The research methods are detailed in the sections that follow:

1.6.1 Literature Survey

In this section the state-of-art survey of existing research work has have been done in securing CR networks is carried out. This involves different security mechanisms (mostly IDS) that have been proposed and developed, why they were developed and which design criteria were used in developing them.

1.6.2 Model Development

After a thorough investigation of the existing work in the literature, the theoretical analysis and representation of model is then presented. This involves the creation of a user model with the intention to define the IDRM security requirements for a distributed, multiuser and dynamic CR network. The intrusion detection and response model (IDRM) is developed afterwards based on the security requirements described.

1.6.3 Proof of Concept

As a proof of concept for this research:

(i) Analysis of the requirements for developing the intrusion detection and response model for CR networks that provides effective and adequate security required in a reliable CR network environment was carried out.

(ii) After the requirement analysis, a prototype IDRM system was developed and implemented, and the results obtained are discussed as shown in chapter 4.

1.7 Research Contribution

The main contribution of the research reported in this thesis to the research community, academia and network security experts is the development and implementation of an intrusion detection and response model (IDRM) to enhance security in Cognitive Radio Networks.

1.8 Research Limitation

The research work reported in this thesis concentrates mainly on the development and implementation of IDRM to enhance Cognitive Radio Network Security. Therefore, no specific attack is implemented as that is not within the scope of the research work.

1.9 Included Publications

Part of the research reported in this thesis has been accepted for publication and another also submitted and is under review by an accredited journal. These papers are:

(i) O Ekabua and O. Ifeoma."Design and Implementation of a Security Framework for Cognitive Radio Networks Resource Management." *International Journal of Computer Science and Information System*, vol12. pp. August, 2012.

(ii) A paper submitted and currently under review in the International Journal of Computer Science and Network Security. The title is: "*Dynamic Management of Data and Information in Cognitive Radio Networks.*"

1.10 Dissertation Summary

The remaining part of this thesis is organized as follows:

Chapter 2 gives a comprehensive literature survey of the existing research work on security in cognitive radio networks mostly IDS. The key terminologies used in this research are also explained.

Chapter 3 provides an analysis of the existing research work on security in CRN, including the investigation on the attacks and vulnerabilities in CRN. The design of the Intrusion Detection and Response Model (IDRM) to enhance security in CRN together with the various requirements for the design and implementation of the IDRM are also presented.

Chapter 4 presents the analysis of the basic requirements necessary for the design and development of the IDRM. Following the basic requirements, an IDRM system was designed and implemented as a proof of concept to validate the research work. The results obtained are also discussed to buttress the model implementation.

Chapter 5 presents a summary, conclusion and recommendations for future work in this research work.

CHAPTER TWO
LITERATURE REVIEW

2.1 Chapter Overview

Spectrum allocation has followed a static policy such that specific bands are assigned to particular users or services operating under license. The huge increase in this new wireless application in the last few years has led to the lack of spectrum for emerging services. Most of the spectrum is vastly underutilized, according to the Federal Communications Commission (FCC) [2, 22].

However, Cognitive Radio Networks (CRNs) are regarded to be a possible solution to this problem by making use of the spectrum left unutilised by the primary users or licenced services. Therefore, secondary users of the spectrum must be capable of identifying white spaces or vacant bands and also select the best portion to operate in while avoiding interferences to primary users [13, 23]. This implies that, whenever the presence of a primary user is detected in the CRN operation channel, the secondary user utilizing the band must switch to another band using a process known as spectrum handoff. Thus, cognitive radio network was firstly defined by Mitola as a "network of cognitive radios". They are smart radios that sense the Radio Frequency (RF) environment using a process known as spectrum sensing to make intelligent decisions based on sensing measurements and stored data thereby selecting the channels with the best conditions and reconfigure them accordingly [5].

CRNs can be classified into decentralized or centralized networks based on whether decisions are taken locally or through a base station which collects information from all nodes. However, in distributed CRNs, decisions are usually taken in an isolated manner by a CR on its own, or in a cooperative way based on the reports provided by a set or all members of the CRN. In other words, sensing information can be exchanged through the data channel (in-band) or by using a dedicated control channel (out-of-band). Apparently, most CRNs may overlap, sharing the spectrum left by primary users which are referred to as self-coexistence. Consequently, there is a need for mechanisms to enable coexistence among existing CRNs [11]. There are a few proposals on CRNs following the different

topologies above mentioned, but most research has focused on the on-going standard IEEE 802.22 for Wireless Regional Area Networks (WRANs). This standard defines a centralized CRN operating in a point-to-multipoint basis, which is formed by a base station and a set of nodes attached to the base station via a wireless link. IEEE 802.22 WRANs are designed to operate in the TV broadcast bands while assuring that no harmful interference is caused to primary transmissions, i.e., digital TV and analog TV broadcasting, and low power licensed devices such as wireless microphones. The set of CRs perform sensing during quiet periods scheduled by the base station, in which any transmission is allowed within the CRN in order to minimize any interference from the WRAN system to the sensing receiver. Sensing information is reported in-band by the CRs to the station, which is responsible for taking the final decision about the existence of a primary user [23].

Although research on CRNs has already been object of a big effort, it is still a hot topic requiring further work, particularly with regard to network security. Like any other wireless network, security in CRN is separated into two lines of defence. The first is focused on avoiding attacks which is usually achieved by means of authentication, authorization, the use of cryptography, and firewall. The second is mostly to detect and identify the attacks that have passed over the first line of defence which is the major aim of intrusion detection and response model (IDRM). However, this research project analyses the existing endeavours in CRN security and investigates vulnerabilities and attacks specific to CRNs. It presents the design of Intrusion Detection and Response Model and specifies the requirements for implementing the IDRM security mechanism to efficiently detect intrusions and generate automated responses to mitigate the intrusions without human intervention [21].

2.2 Key Terminologies: The key terminologies used in this research project are explained below.

(a) Cognitive Radios

Cognitive radios are smart radios which are capable of identifying spectrum bands (radio frequencies) which are not being utilized and which automatically tune to that frequency

to receive or transmit signals. This capability is called spectrum sensing and it is achieved via dynamic spectrum access (DSA) [2].

(b) Cognitive Radio Networks

Cognitive radio networks (CRNs) are an improvement on wireless communication (traditional and conventional radio and software radio) to be able to maximize, and optimize spectrum resources (white space), due to its capability to actively detect and allocate the resources on its own [2].

(c) Security

This means "protecting systems, data and information from unauthorized access, use, disclosure, disruption, modification, or destruction," according to a specified or outlined policy. Security forms the vital aspect of cognitive radio networks; hence this research focuses mainly on intrusion detection and response model as two important aspects that must not be excluded in cognitive radio networks security infrastructure to provide advanced protection and ensure quality of service [24].

(d) Intrusion Detection

This consists of procedures and systems created and operated to detect system intrusions and intruders. Intrusion detection monitors all the network activities in order to detect the intrusions. It searches for security violation incidents, recognizes unauthorized accesses, and identifies information leakages within the CRNs environment [25].

(e) Response Model

This is a specified procedure that is developed to generate a quick response to detected intrusions or system violations because system administrators neither can keep up with the pace that an intrusion detection system is detecting intrusions, nor can they react within adequate time limits. A response model is an automatic response system that has to take over this task by reacting without human intervention within the cognitive radio network [26, 27].

(f) Spectrum Resources

In cognitive radio technology, spectrum band and frequency transmitted via the spectrum nodes forms the spectrum resources. Spectrum resources are unique national and International resources that are limitless and infinitely renewable. A component of a system that provides or hosts services, which are managed based on a set of rules and regulations is collectively referred to as a service policy. Access to a resource is either enforced by the resource itself or by the policy enforcement point, protocol, router or gateway. This is located in between the resource and the requester, in order to protect the resource form unauthorized access. It is regulated by the policy decision point (PDP) and determined by the policy enforcement point (PEP). In other words, a resource can also be referred to as a service [28].

(g) Intruders

Intruders are referred to as "attackers" who have the knowledge and skills in certain sophisticated tools used to compromise or violate a CRN security system. They gain unauthorized access into the network with the intention to modify, fabricate, interrupt or intercept data packets and information going in and out of the networks for some financial gains or selfish motives [16].

2.3 Related Work

- IEEE 802.22 – There has been ongoing research in the IEEE 802.22 standard in the past few years for Wireless Regional Area Networks (WRANs). This standard defines a centralized CRN that operates in a point-to-multipoint basis which is formed by a base station and a set of nodes that are attached to the base station through a wireless link. The IEEE WRAN are majorly designed to operate in TV broadcast bands, while ensuring that no form of interference is caused in the primary users and transmissions which include digital and analog TV broadcasting, and low power licensed devices such as wireless microphones.

- RFC1024: Internet Standard Management Framework, also known as Simple Network Management Protocol traces its root back to the Simple Gateway

Management Protocols (SGMP). It has since its development evolved into series of versions up to SNPV3 [RFC270]. In Wireless Ethernet and WI-FI, several numbers of standards and technologies for wireless LAN which are supported by cognitive radio technologies includes LAN 802.11 and others.

Presently, IEEE802.11b standard also called Ethernet and WI-FI is getting more wide range deployment. It transmits an unlicensed radio spectrum at 2.49HZ and provides wireless Ethernet access at 11Mbps.This standard defines the physical layer and media access control (MAC) layer and any wireless local area network. The physical layer uses direct sequence spread spectrum (DSSS) which spreads the energy in a signal over a wider frequency range, thus improving the ability of the receiver to recover original bits transmitted [21,29].

In the world of security, we may face a number of threats from attackers, from misconfiguration of infrastructure or network-enabled devices, or even from simple unavailability or decrease in quality of service as a result of unpredicted behavior of the network. The majority of the world today has become network dependent and as such when any loss of network connectivity and loss of services provided by such networks is encountered, the users are bent to suffocate and this can be potentially devastating to any business, organization or company.

Therefore, mechanisms for protecting networks and various infrastructures or devices that support the networks must be put in place to achieve an efficient quality of service. This is the essence of network security and the interest of this research. Avenues to protect cognitive radio network must include intrusion detection and response model in other to achieve maximum security standard [8].

The basic intrusion detection principles are based on the understanding that intrusion activities are noticeable and can be differentiated from other normal ones and therefore are detectable [30]. Many intrusion activities have been proposed in literature. Depending on the technique used, these approaches are classified into three categories namely: misuse detection, anomaly detection, and specification-based detection (stateful protocol analysis or stateful packet inspection [31]. It was stated by Endorf that when James

Anderson came up with a technical report for the U.S. Air Force, intrusion detection was introduced as a formal research and thus has been followed up by many researchers until present day [32, 33].

The first intrusion detection expert system (IDES) was proposed in the 1980s. The research proposed the use of profiles in monitoring using statistical metrics and models to establish where anomalous events or malicious activities have occurred. This made gathering statistical data for inferring systems profiles become a popular area for researchers in the 1980s. Intrusion detection system uses statistical method to characterize audit trail data into features. Haystack was able to reduce large quantities of audit data by delivering the summaries of the behaviors and attitudes of the user to be analyzed by the system or network security management. This proposal was sponsored by the U.S. Air Force cryptologic support center. This is to aid the security officers to detect intrusion in Air Force multiuser computer system [18].

Apparently, a few other similar systems function in batch-mode and utilize statistical analysis using expert systems to gather anomalous activities. Multics intrusion detection and alert system (Midas) from the national computer security centers (Ncsc) and network audit director and intrusion reporter (Nadir) are examples. Nadir monitored a computer network mode of trail from network activities while the others took audit logs from monitoring hosts as their source of data [18].

However, the early 1990s was the beginning of network intrusion detection where a team of security analysts introduced the idea of intrusion detection in their paper. The study on developing IDS in a broadcast environment was proposed and Ethernet was described in the paper [8]. Collecting data from local areas networks, profiles on usage of network resources could be hierarchically developed. These profiles were used as patterns to identify security violations. Commercial IDS emerged with Haystack research, developing Haystack host-based stalker product [18].

Zang et al proposed distributed intrusion detection and response system that is able to detect signs of intrusion locally and independently, while neighboring nodes can investigate collaboratively in a wider range [20].

Albers et al proposed a distributed and collaborative architecture of IDS. The architecture uses mobile agents for its analysis and detective activities. It implements a local intrusion detection system on each node which is extended to the global level by means of common cooperation [19]. In addition, Sterne et al proposed a dynamic intrusion detection hierarchy. The system is potentially scalable networks using clustering. It is clustered into two levels where the first level forms the cluster heads and the second level forms the leaf level nodes. Each of the nodes has the capability to monitor, log, analyze, respond and alert to the cluster heads [34]. More so, Kachirski et al proposed a multi-sensor intrusion detection system. The proposed system is based on mobile agent technology and can be separated into three modules where each of the modules represents a certain functionality of the mobile agent [35].

Internet security system (ISS) came up with its network intrusion detection system called Real Secure. Cisco participated in the market with its product - Net Ranger directed by Cisco acquiring wheel team. Martin Roesch surfaced with Sourcefire in the new millennium, bringing the popularity of Snorf, which made Snorf become one of the leading open source products that specializes in network intrusion detection using a pattern-matching algorithm to perform misuse detection on network data packets.

Basically, CRNs are expected to offer solutions to the problem of spectrum scarcity through fair use of the vacant spectrum bands. As a result of the wireless nature of the CRNs, it faces all common security challenges associated with other wireless networks. This has made it prone to several attacks targeting the various network layers including the physical and medium (MAC) access layers [36]. Such attacks include IP spoofing, sniffing, denial of service (DoS), license user emulation and others [37, 38]. Previously an IBM monitoring tool known as Distributed Wireless Security Auditor was being used to police the activities that go on in most networks.

However, this research project has proposed intrusion detection and response model (IDRM) to enhance security in cognitive radio network to introduce a more effective and efficient means to carryout network security checks to detect the malicious activities that increase on daily basis [8]. Moreover, the essence of IDRM is to achieve the most common security objectives for wireless networks which include: (i) confidentiality

which ensures that network data cannot be read by unauthorized users, (ii) integrity which ensures that data transmitted in and out of the network are not intentionally or unintentionally changed on transit, (iii) availability which ensures that network users (device and individuals) are able to access network resources whenever needed, and (iv) access control which ensures that network's resources are restricted to only the authorized users only. Apparently, in the effort to achieve the security objectives, a reliable security infrastructure is developed which guarantees adequate quality of service (QoS) and a substantial increase in the demand for CRNs services [39].

2.3.1 Intrusion Detection Concept

Intrusion detection consists of procedures and systems developed and operated to detect system intrusions. Most system research is concerned with designing robust architecture for intrusion detection systems. However, it has been discovered that the most difficult aspect of the system design is the decision on the appropriate location for the intrusion detection system in the network. A direct inspection of the condition and state of the monitored system in real time provides a better visibility which makes detection more effective and increases the range of analysable events. This effectiveness is evaluated based on the decrease in the risk of having an incorrect view of the system and the chances of having an unmonitored attack [18].

2.3.2 Intrusion Detection Systems

Intrusion detection systems (IDSs) provide a solution to the problem of intrusions that is militating against wireless networks on daily basis. They are systems that monitor the entire network assets and are capable of detecting anomalous behaviors or misuse and sometimes alerts the management to take corrective action, an example is a burglar alarm. They are designed to provide the instance, method, source, and attack signature of a particular intrusion. All IDS operate as host based or, network based, which forms the main types of IDS. IDS have been expressed in several ways for commercial competence but operate using any of the three methods which includes: (1) signature based (2) anomaly based and (3) specification-based (stateful packet inspection or stateful protocol analysis).

(1) Signature based

The intrusion detection scans network packet for specific byte sequences (signatures) that are already stored in the networks database of known attacks. Depending on the way signatures are detected, they have been defined and named as follows: Rule based, Expert system, State models, String match.

However, there exist some commercial signature based application systems such as:

(a) Pattern Matching

The intrusion detector searches for known attack patterns that have been previously encountered and can be coded for further reference. For instance, if an IPv4 packet with destination port 2345 has the string 'smash' (some signature) in the payload, a flag or indication then arises. An alarm is then sent to the administrator indicating that an intrusion has occurred. This is the simplest method of intrusion detection but it is highly specific, and can raise a number of false alarms and missed variants. It is based on packet sniffing and not very useful in case of stream-based traffic.

(i) Stateful Pattern Matching

This is a slight improvement of the pattern matching that takes the responsibility for signature split in the data packets. It maintains the states of the packets and it is also applicable to stream-based traffic. For instance, if the string 'smash' is being looked for and it is split into 'sma' 'sh' in consequent packets. It is looked for and detected as intrusion.

(ii) Protocol Decode-Based Analysis

This is a kind of intelligent extensions to pattern matching approach. The protocol elements are identified alongside with other known patterns. Other variable fields such as number of arguments, length of field and others are also considered. A good example is the protocol decoding which is helpful in limiting the beginning and end points of a pattern search where variable fields are encountered.

(2) Anomaly Based

Anomaly based detectors are made to look for network traffic deviating from models of past 'normal' behavior. But they look for known attacks as well, e.g. when some process (e.g. a Trojan) tries to write to the registry under Windows NT system files. This behavior is abnormal and can be flagged as an anomaly. These detectors are found in applications in the following forms:

(a) Protocol Anomaly

This looks for deviations from standards defined in RFC's. But they are useless with poorly understood or complex protocols.

(b) Traffic Anomaly

In traffic anomaly the detector is configured to look for unusual traffic activities, such as flood of packets, preventing Denial-of-Service attacks.

(c) Statistical Anomaly

The detector is configured to identify statistical baseline normal traffic activity and alerts are expected when deviations are identified. More so, statistical anomaly detection systems are described by commercial software as behavior measure intrusion detectors and are further categorized into three classes such as; event count based, interval based and resource consumption based. Event based includes operational count, mean and standard deviation, Markov process model - Interval times based includes multivariate model and resource consumption based includes time series model.

(3) Specification-based

This intrusion detection method monitors current behavior of systems according to specification that describe desired functionality for security-critical entities. A mismatch between current behavior and the specifications is reported as an attack or intrusion. This process compares predetermined profiles for each protocol state against observed events to identify deviations. [40].

2.3.3 Types of IDS

Intrusions detections are basically of two types depending on how they monitor activities. They include host-based and network-based.

(i) Network-based IDS (NIDS)

Network IDS is a dedicated monitoring component on a network and can be placed inside a firewall or outside it or at the perimeter of the system boundary. It resides on computer or appliance connected to a segment of an organization's network and looks for signs of attacks. When examining packets, NIDS looks for attack patterns. It is usually installed at a specific place in the network where it can watch traffic going into and out of particular network segment in order to detect an attack.

This is achieved by using special implementation of TCP/IP stack. In the process of protocol stack verification, NIDSs look for invalid data packets. In application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use. Good network design and placement of NIDS can enable organizations to use a few devices to monitor large networks. NIDSs are usually passive, so they can be deployed into existing networks with little disruption to normal network operations.

(ii) Host-based IDS (HIDS)

Host IDS is a monitor on the host computer only, usually placed at business critical hosts and external facing servers. It resides on a particular computer or server and monitors activity only on that system. It can benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes files. Most HIDSs work on the principle of configuration or change management. It is usually installed so that it can access information encrypted when traveling over a network. It can detect local events on host systems and detect attacks that may elude a network based IDS. It is most effective on a host system, where encrypted traffic will have been decrypted and is available for processing. It is not affected by use of switched network protocols and can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs [41].

2.3.4 IDS Architecture

Whether it is a host or network-based IDS, it will typically consists of several specialized components working together to achieve a common goal. These components are often logical and software-based. These logical components include traffic collector, analysis engine, signature database and user interface and reporting.

2.3.5 Logical IDS Component

Several components constitute the IDS, making it a functional entity. Figure 2.1 depicts the different entities making up the intrusion detection system.

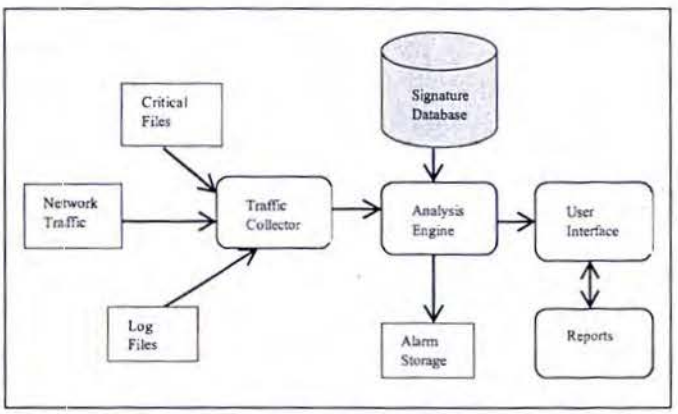


Figure 2.1 Logical IDS Component [42]

(i) Traffic Collector

This component of the IDS collects information and events for the IDS to examine. This information, activities or events could be log files, audit logs, or incoming and outgoing traffic on a specific system. In network-based IDS, the traffic collector (component) is a mechanism for coping traffic outside the network link. It is specifically designed to pull traffic from the network. This component usually behaves like a network traffic sniffer, every packet transmitted along its duty path off the network to be properly examined.

(ii) Analysis Engine

This component examines the network traffic that has been collected by the traffic collector. It is regarded as the most important component of the IDS due to its responsibility. It is often referred to as the brain of the IDS. It decides the activity, communication, transmission or access that is granted or denied. It is a decision or pattern matching mechanism. It compares the traffic and information supplied to it by the traffic collector against known attack patterns stored in the signature database. If the activity matches any known pattern, it reacts to it as an intrusion by generating an alarm. This examination of traffic is done as quickly as possible to enable IDS to react against attacks in real time.

(iii) Signature Database

This is a collection of predefined attack patterns (suspicious or malicious activities), that have already been defined and classified in the network. They indicate suspicious activities and real attacks. Once the analysis engine examines traffic, it matches the pattern with the appropriate signature in the database. It can contain as many signatures as possible depending on the storage capacity provided.

(iv) User Interface and Reporting

This is the visible component of the intrusion detection system. It interfaces users (the human elements) by enabling the humans to interact with the network regardless of the complexity and type, changing parameters, receiving alarms, tuning signatures and response patterns [42].

2.3.6 IDS Products and Vendors

An intrusion detection system (IDS) monitors and analyses traffic to detect signs of attempted intrusion by attackers. They can detect a variety of attacks in progress as well as attempts to scan the network for weaknesses. However, IDS can be a dedicated appliance or a software solution that can monitor a single host. Table 2.1 provides a list of some of the currently available IDS products and vendors. The table provides the name

(vendor), the product and a link on where to find more information about the product. Some of these products are free while some are obtained on specific charges [42].

Table 2.1: List of IDS vendors and products

Name	Product	Where to find more information
Cisco Systems, Inc.	Cisco IDS	www.cisco.com
Computer Associates	e Trust	www.ca.com
Enterasys Network	Dragon	www.enterasys.com
Internet Security Systems, Inc.	RealSecure	www.iss.net
Intrusion, Inc.	SecureNet, SecreHost	www.imtrusion.com
Intruvert Networks	IntruShield	www.intruvert .com
iPolicy Networks	ipEnforcer	www.ipolicynetworks.com
NetScreen	NetScreen IDP	www.netscreen.com
NFR Security, Inc.	NFR	www.nfr.com
Snort	Snort (free, open source)	www.snort.og
Symantec Corporation	Intruder Alert	www.symantec.com
TippingPoint Technologies	UnityOne	www.tippingpoint.com
Tripwire, Inc.	Tripwire	www.tripwiresecurity.com

2.4 CRNs-First Line of Defence

The major objective of security in cognitive radio-based wireless networks is to provide a secured and reliable computational environment and effective quality of service. Apparently, security measures such as authentication, authorization and firewall and access control mechanisms provide the first line of defense in cognitive radio networks [30].

(i) Authentication

Authentication is a security measure in Cognitive Radio Networks (CRNs). It ensures that entities (users) are truly who they claim to be. This is verified before access to the network is granted. It actually associates a unique identity to each user in CRN, such as user identification name or password as approved by the service security policy. Using these unique forms of identification clients (users) can freely request for the spectrum resources. It involves the process of verification and validation of users' identity (ID).

(ii) Authorization

Authorization is a security measure that allows access to only the right entities (users) having the approved privilege to the particular resources requested. Different forms of authorization exist, such as out band authorization, signature authentication and password authentication. Moreover, for any communication (interaction or conversation) involving different parties or entities exchanging information, there should be a mutual trust relationship across the multiple domains in CRNs.

(iii) Access Control

Access control is a security capability for monitoring and controlling access to the limited spectrum resources, dynamically managing data and information in CRNs, for a secured communication and quality of service (QoS). This allows users to have access to only the CRNs resources for which they are authorized to access.

(iv) Firewall

Firewalls are mechanisms for maintaining control over the traffic that flows into and out of our network. They are used to prevent intruders from having access to the organizations network. It is typically placed in a network where the level of trust change is seen. A firewall can be placed on the border between our internal network and the internet. It can also be placed on our internal network to prevent network traffic of a sensitive nature from being accessed by unauthorized users. The concept of firewalls is basically to examine the packets that are coming in and out of the network in order to determine what should be allowed in or out. The complexity and configuration of the

firewall determines whether traffic is allowed or blocked. For instance, a firewall might allow or disallow traffic based on the protocol being used, allowing Web and e-mail traffic to pass, but blocking everything else [30]. However, attackers have become skilled in the use of sophisticated tools to penetrate the first line of defence. This has necessitated the interest of this research work.

2.4.1 Types of Firewall

Firewalls are of different types which include: packet filtering, stateful packet inspection, deep packet inspection, and software firewalls. They are used based on the specification and requirements of the system and network.

(i) Packet Filtering

Packet filtering is one of the oldest and simplest of firewall technologies. Packet filtering looks at the contents of each packet in the traffic individually and makes a gross determination, based on the source and destination IP addresses, the port number, and the protocol being used, and also whether the traffic will be allowed to pass or not. Each packet is examined individually and not in concert with the rest of the packets comprising the content of the traffic, it can be possible to slip attacks through this type of firewall.

(ii) Stateful Packet Inspection

This is generally referred to as stateful firewalls. It functions on the same general principle as packet filtering firewalls. They are slightly different in the sense that, they are able to keep track of the traffic at a granular level, whereas a packet filtering firewall only examines an individual packet out of context. A stateful firewall is able to watch the traffic over a given connection, generally defined by the source and destination IP addresses, the ports being used, and the already existing network traffic. It uses what is a state table to keep track of the connection state and will only allow traffic that is part of a new or already established connection.

(iii) Deep Packet Inspection

This type of firewall added another layer of intelligence to the firewall capabilities. Deep packet inspection firewalls are capable of analysing the actual content of the traffic that is flowing through them. Packet filtering firewalls and stateful firewalls concentrate at the structure of the network traffic itself in order to filter out attacks and undesirable content, deep packet inspection firewalls can actually reassemble the contents of the traffic to look at what will be delivered to the application for which it is ultimately destined. Although this technology has great promise for blocking a large number of the attacks, the question of privacy is also raised. In general, someone in control of a deep packet inspection device could read every one of our e-mail messages, see every web page exactly as we saw it, and easily listen in on our instant messaging conversations.

(iv) Software Firewalls

Software firewalls are a very useful additional layer of security we can add to the hosts residing on the host system or networks especially when they are properly configured. This type of firewall generally contain a subset of the features and can be found on a large firewall appliance but are often capable of performing similar functions with packet filtering and stateful packet inspection. The rule sets of such applications are often expressed in terms of the particular applications and ports allowed to send and to receive traffic on the various network interfaces that exist on the host. Software firewalls ranges from the relatively simple versions that are built into chip with common operating systems for large versions intended for use on corporate networks which include centralized monitoring and the capability for considerably more complex rules and management options.

However, attackers are getting more knowledgeable by day and as such, attackers are getting more sophisticated by the use of sophisticated tools such as sniffers and scanners. These tools enable intrusions to bypass the first line of defence. We must not fold our arms and watch the dividends of this promising wireless technology- CRN being overtaken by these attacks. Consequently, this has necessitated the main goal of this research work which is to design an intrusion detection and response model to enhance

security in cognitive radio networks. The IDRM is designed and implemented to generate automated responses capable of detecting intrusions and warding off intruders without any form of human intervention. [7].

2.5 Cognitive Radio Network Architecture

It is necessary to also introduce the general design of the CRN architecture and other relevant components of the network for a broad view and understanding of the concept since this is the architecture (foundation) upon which this research project work is build on. Cognitive Radio Network is dynamic and adaptive in nature. The architecture of CRN in Figure 2.2 shows vividly the different components of the CR network, both functional, operational, and hardware, together with the relationship between them. The spectrum band is infinitely renewable, though limited due to its high demand by the secondary users.

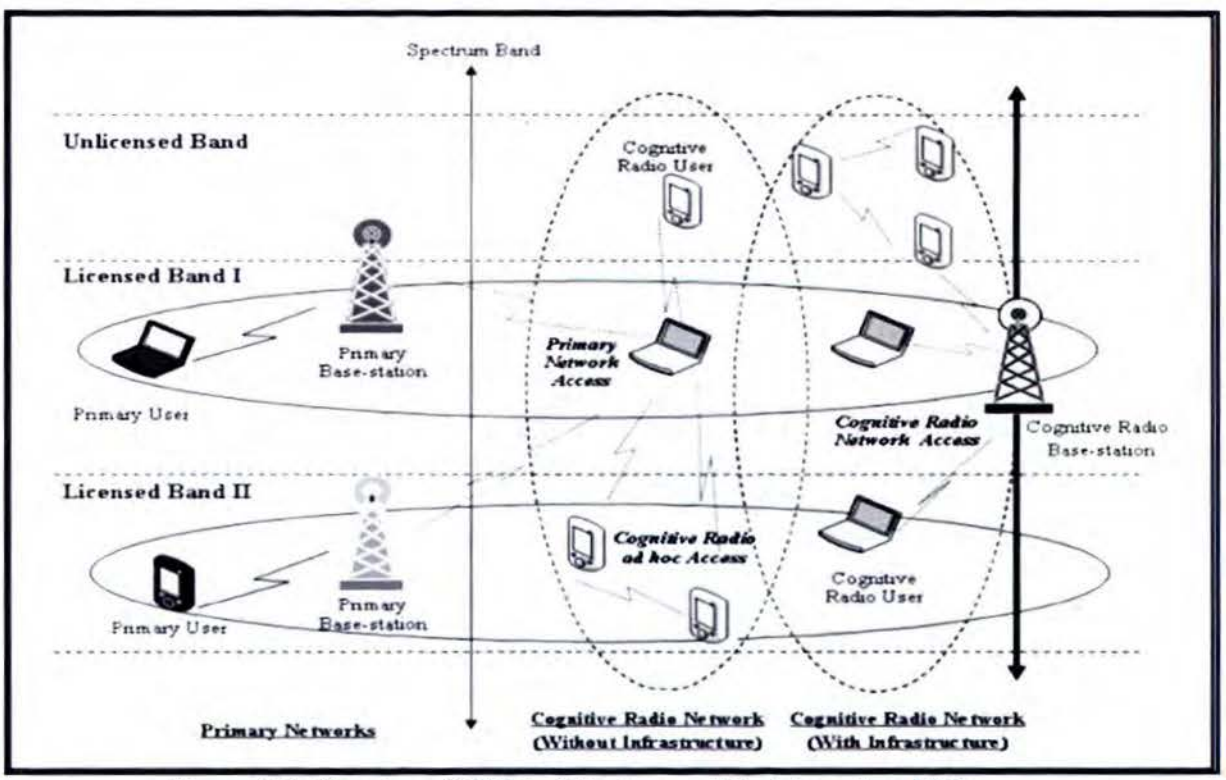


Figure 2.2: Spectrum CRN Architecture and its Interaction [43]

The Primary network has the legitimate right to a certain spectrum band, whereas cognitive networks do not have the license to operate in a choice band. The primary and

unlicensed networks consist of some basic elements which include primary user, primary base station, cognitive radio user, cognitive radio base station, cognitive radio network access, cognitive radio ad hoc access and primary network access.

However, the Primary user has the license (right) to operate in a specified spectrum band. This access right can be only controlled and monitored by its base-station and unauthorized users should not interfere or affect its operations. Consequently, the primary base-station is a fixed wireless infrastructure network component that has a spectrum license but does not have any capability for cognitive radio to share the spectrum with other users of cognitive radio. Therefore, the primary base-station may need to have both the primary and cognitive radio protocols to enable primary network access for the cognitive radio users.

Moreover, the spectrum access is allowed for the cognitive radio users only when not occupied by the authorized users because they do not operate with the spectrum license. Therefore, the cognitive radio user capabilities such as spectrum sensing, spectrum decision, spectrum handoff and cognitive radio MAC, routing and transport protocols are required to enable communication with the base-station and other cognitive radio users as well.

The cognitive radio base-station is a fixed wireless infrastructure component that has cognitive radio capabilities and provides single hop connection to cognitive radio users without the license for spectrum access. The cognitive radio users communicate with each other either in a multi hop manner or access the base-station. Consequently, the cognitive radio network architecture in Figure 2.2 consists of three different types of network access such as: cognitive radio network access, cognitive radio ad hoc access and primary network access having different implementation requirements. However, in cognitive radio network access, cognitive radio users (secondary users) have the capability to access the cognitive radio base-station in both the licensed and unlicensed spectrum bands. The entire interactions take place inside the cognitive radio network; therefore the access scheme does not depend on the primary network. In ad hoc access cognitive radio users communicate with each other on both licensed and unlicensed spectrum bands via ad hoc connection. They are also capable of building their own access

technology through which they can communicate. In primary network access, when the primary network is dormant, the cognitive radio users are able to access the primary base-station via the licensed band [43].

2.6 Components of Cognitive Radio Network

Cognitive radio networks are majorly classified into two groups which are network components and functional components.

2.6.1 Network Components

The CRNs components consist of two groups which are the primary network and the cognitive radio network. The primary network group or licensed network is referred to as an existing network. The primary users are those who have the license (the right of access) to operate within the spectrum band of the existing network. They are given the first priority in access to spectrum. If primary network is infrastructure based, primary user activities are controlled via primary base stations. This is also called centralized network.

The cognitive radio network is a secondary network and does not have the license to operate in a choice spectrum band so an additional component is required to enable them share the licensed spectrum band conditionally. They can also use base stations with a single hop transmission, connecting the cognitive radio networks in their different locations. They are referred to as unlicensed users or secondary user. They take the next priority in access to spectrum band. The cognitive radio network is also called decentralized network due to the fact that they can cluster in different geographical locations.

Generally, cognitive radio networks are dynamic in concept. This dynamic nature makes them vulnerable to attacks, which results into huge security challenges. However, spectrum brokers are deployed to distribute the spectrum resources in other to dynamically and effectively manage the flow of data and information in CRNs, and also efficiently control access to spectrum bands to avoid collision of users, and network failures.

(1) Spectrum Heterogeneity

The cognitive radio networks have two types of operational bands which are licensed band operation and unlicensed band operation. The licensed band is primarily occupied by the primary users. Cognitive radio networks have the capability to operate and access both the licensed part and the unlicensed part. Secondary users are capable of accessing both the licensed (used by primary user) and unlicensed part of the spectrum band using wideband access technology. Therefore, cognitive radio networks are majorly focused on detecting the position of primary users per time to be able to access the spectrum band, exercising the same access right to the spectrum band. Consequently due to spectrum heterogeneity, sophisticated spectrum sharing methods are required for cognitive radio users to compete with the unlicensed band.

(2) Network Heterogeneity

This is a characteristic of CRNs that allows cognitive radio users to perform three different access types which are cognitive radio network access, cognitive radio ad hoc access and primary network access.

(i) Cognitive Radio Network Access

In this type of network access, cognitive radio users can access their own cognitive radio base station while on both licensed and unlicensed spectrum bands. The reason is because all interaction occurs inside the cognitive radio network and the own spectrum sharing policy is independent of the primary network and is not location sensitive. Centralized networks make use of this type of access. They are separated into cells and the cells are managed by secondary based stations which control the medium of access. The secondary users (unlicensed users) operate together with their base stations performing periodic spectrum sensing activities. The secondary base stations are interconnected using a wired backbone which is usually infrastructure –oriented

(ii) Cognitive Radio Ad hoc Access.

Cognitive radio users (secondary users) are able to communicate with other cognitive radio users in an ad hoc manner on both licensed and unlicensed spectrum. Decentralized

networks users make use of this type of access. The users are not interconnected by any infrastructure. Communication among the secondary users is done in an ad-hoc manner. Two or more users within a close range can exchange information directly while the ones not within a close range (across huge geographical areas) can exchange information using a medium or link called multiple or single hops. However, spectrum sharing network is a sub class of decentralized cognitive radio network whereby two wireless networks coexist in an unlicensed band. A very good example of this is the coexistence of IEEE 802.11 and IEEE802.16. They utilize a common spectrum coordination channel (CSCC) developed to control exchange of information on transmitter and receiver parameters.

(iii) Primary Network Access

This is different from other network access types because the users access the network using an adaptive MAC protocol which supports roaming over multiple primary networks with different access technologies [43].

2.6.2 Functional Components for Spectrum Management in CRNs

Cognitive radio network emerged with improvements which give it an edge over conventional cognitive and wireless networks. It is highly distinguished and, efficient by its services and functions such as:

(i) Spectrum Sensing

One of the major characteristics and requirements of cognitive radio network is that, it is capable of scanning the spectrum band, identifying unutilized channels available for opportunistic transmission. This is referred to as spectrum sensing. Primary user network and secondary user network are separate from each other and therefore, do not receive any direct feedback from each other as regards transmission. The secondary user relies so much on their individual or cooperative sensing capability to detect primary user transmission. Since the primary users are widespread, occupying a large geographic location, it becomes quite a difficult task for secondary users to sense the entire spectral band depending on weak primary signals to determine their presence [43].

(ii) Spectrum Analysis and Decision

Each spectrum band possesses various distinctive features and attributes which are unique to them as a result of the number of user (primary and secondary), and the frequency range. Spectrum sensing identifies a list of spectrum bands which are available and not occupied by the primary users (available band listed) which can be utilized. Based on the availability of spectrum, channels can be allocated to cognitive radio users. The allocation does not depend totally on the spectrum availability but also on internal (and external) policies. This evaluation process is called spectrum analysis and decision. Some of the characteristics and features of spectrum bands that are used to evaluate their effectiveness are interference, path loss, wireless link errors, link layer delay, and holding time (expected duration for the secondary user to occupy the spectrum band) [43].

(iii) Spectrum Sharing

Due to the nature of cognitive radio network which allows multiple cognitive radio users to access the spectrum, cognitive radio network should then be coordinated to prevent multiple users colliding in overlapping areas of the spectrum. This coordination activity is called spectrum sensing [43].

(iv) Spectrum Mobility

The ability of cognitive radio network to dynamically switch between spectrum accesses is known as spectrum mobility. Secondary users are not granted constant spectrum access within the licensed bands. Spectrum band availability changes overtime as a result of this. Consequently, cognitive radio network considers spectrum mobility in designing spectrum protocols.

Spectrum mobility usually experiences some delay in handoff time (the time taken by secondary users to release the spectrum for primary users). This is incurred within the time difference between the secondary network detection of primary transmission and secondary users quitting the spectral band. The Federal Communication Commission (FCC) has created upper bounds on the spectrum handoff duration to monitor and control extended interference to primary users [43].

2.7 Capabilities of Cognitive Radio Networks

The capabilities of cognitive radios as nodes of CRN can be classified based on their functionalities such as cognitive capability, self-organized capability and reconfigurable capability

(a) Cognitive Capability: This refers to the ability for a cognitive radio to sense the environment which includes:

(i) Spectrum Sensing

A cognitive radio can sense spectrum and detect "spectrum holes" which are those frequency bands not used by the licensed users or having limited interference with them.

(ii) Spectrum Sharing

A cognitive radio could incorporate a mechanism that would enable sharing of spectrum under the terms of an agreement between a licensee and a third party. The parties may eventually be able to negotiate for spectrum use on an ad hoc or real-time basis, without the need for prior agreements between all parties.

(iii) Location Identification

This is ability to determine cognitive radio location and the location of other transmitters, and then select the appropriate operating parameters such as the power and frequency allowed at its location. Bands such as those used for satellite downlinks are receive-only and do not transmit a signal. Location technology can be an appropriate method of avoiding interference because sensing technology will not be able to identify the locations of close by receivers.

(iv) Network/System Discovery

For a cognitive radio terminal to determine the best way to communicate, it shall first discover available networks around it. These networks are reachable either via directed one hop communication or via multi-hop relay nodes. For example, when a cognitive radio terminal has to make a phone call, it shall discover if there is GSM BTSs or WiFi

APs nearby. If there is no direct communication link between the terminal, the BTSs/APs and other cognitive radio terminal access networks are reachable, it can still make a call in this circumstance. This ability to discovery one hop or multi-hop access networks is important.

(v) Service Discovery

This is usually accompanied with network/system discovery. Network or system operators provide their services through their access networks. A cognitive radio terminal finds appropriate services to fulfil its demands.

(b) Reconfigurable Capability

This is the ability to adapt to the environment. It includes frequency agility, dynamic frequency selection, adaptive modulation/coding, and transmit power control.

(i) Frequency Agility

It is the ability of a radio to change its operating frequency. This ability usually combines with a method to dynamically select the appropriate operating frequency based on the sensing of signals from other transmitters or on some other method.

(ii) Dynamic Frequency Selection

It is defined in the rules as a mechanism that dynamically detects signals from other radio frequency systems and avoids co-channel operation with those systems. It consists of methods that a device could use to decide when to change frequency or polarization. This could include spectrum sensing, geographic location monitoring, or an instruction from a network or another device.

(iii) Adaptive Modulation/Coding

Adaptive modulation techniques can modify transmission characteristics and waveforms to provide opportunities for improved spectrum access and more intensive use of spectrum while "working around" other signals that are present. A cognitive radio could

select the appropriate modulation type for use with a particular transmission system to permit interoperability between systems.

(iv) Transmit Power Control

Transmit power control is a feature that enables a device to dynamically switch between several transmission power levels in the data transmission process. It allows transmission at the allowable limits when necessary, but reduces the transmitter power to a lower level to allow greater sharing of spectrum when higher power operation is not necessary.

(v) Dynamic System/Network Access

For a cognitive radio terminal to access multiple communication systems/networks which run different protocols, the ability to reconfigure itself to be compatible with these systems is necessary.

(c) Self-Organized Capability

This is the ability to analyse and learn sensed information. It consists of the following:

(i) Spectrum/Radio Resource Management

To efficiently manage and organize spectrum holes information among cognitive radios, good spectrum management scheme is necessary.

(ii) Mobility and Connection Management

Due to the heterogeneity of CRNs, routing and topology information is more and more complex. Good mobility and connection management can help neighbourhood discovery, detect available internet access and support vertical handoffs, which help cognitive radios to select route and networks.

(iii) Trust/Security Management

Since CRNs are heterogeneous networks in nature, various heterogeneities (e.g. wireless access technologies, system/network operators) introduce lots of security issues. Trust is thus a prerequisite for securing operations in CRNs [43].

2.7.1 Features of Cognitive Radio Network Capability

This explores the potential levels of cognitive ability. Cognitive radio network allocates intelligence between the wireless and the mobile units. It utilizes a model based reasoning to sense its environment, location, networks, protocols, users and its inbuilt internal structure. Cognitive radio network is aware of the users communication needs and the Table 2.2 specifies the various components of the capabilities and the corresponding cognitive task of CRN [43].

Table 2.2: CRN Capability Features

Capability	Cognitive Task
Pre-programed	The radio has no model-based reasoning capability.
Goal-driven	Goal-driven choice of RF band, air interface and protocol.
Context Aware	Determines external context (minimum user involvement).
Radio Aware	Flexible reasoning about internal and external network.
Capable of planning	Reasons over goals as a function of time, space, and context.
Conducts negotiations	Express competent plans to peers and network.
Learns Fluent	Autonomously determines the structure of the environment
Adapts plans	Autonomously modifies planning as learns fluent changes.
Adapts protocol	Autonomously propose and negotiates new protocols.

2.8 CRN Protocol Layers

Cognitive radio network has reconfiguration as a special characteristic that is able to influence all the protocol layers due its nature of dynamic spectrum access [5].

(i) Physical layer in cognitive radio networks

The physical layer operates on the data transmission directly through the physical medium. The major difference between the physical layer of the cognitive radio network and other conventional network is the spectrum sensing. It is an important part in cognitive radio networks and its main function is to detect the spectrum holes (vacant spaces) for data packet transmission. The information from spectrum sensing enhances spectrum decision. Once the license user appears, reconfiguration automatically takes place which obviously changes operation parameters such as frequency, power and modulation in order to adapt to the new operating spectrum [5].

(ii) Link layer in cognitive radio networks

The link layer forms the data and regulates the access to the physical resources. Several differences exist between the link layer of the conventional wireless network and cognitive radio network. The characteristic of communication channels in CRN are different from the conventional networks. The users in conventional wireless networks have fixed channels to use which are according to their protocols, while, in CRN the channels are not fixed which means that it can exist anywhere in the whole spectrum due to accessing the spectrum dynamically. Another difference is that cognitive radio users always transmit data simultaneously using multiple channels in order to increase the throughput. Therefore, MAC (media access control) scheduling becomes an important means to maintain the channel's utilization in order to avoid data collision [5].

(iii) Network layer in cognitive radio networks

The Network layer handles the routing, and routing scheme is more complicated in CRNs. The paths are designed directly by the router in conventional wireless networks. Data is transmitted from the source and delivered to the destination along the designed path in the network, while, in CRNs it is quite different because the spectrum can be accessed freely. Therefore, reconfiguration information largely influences the routing scheme and communication performance is directly affected by the spectrum. However, in order to handle the routing problem in CRN a cross layer solution is proposed to enhance the efficiency of the transmission. The solution suggests that, the routing algorithm and the spectrum management be considered together to make decisions for the channel scheduling instead of the router's making decisions directly [5].

(iv) Transport layer in cognitive radio networks

The transport layer is a control layer that majorly handles flow control, error control, and congestion control. The two main protocols at the transport layer are the UDP (User Datagram Protocol) and the TCP (Transport Control Protocol) which requires changes in order to adapt to CRNs. The two important factors involved in the transport layer such as the round trip time and the packet loss probability are influenced by the characteristics in CRNs such as spectrum sensing technology, operating frequency, interference level and

availability bandwidth. For instance, it takes some time for a particular transmission to change from one channel to another due to the reconfiguration that takes place in CRNs. However new transport protocols are been designed to adapt to these changes since the conventional protocols for transmission in fixed channels are not appropriate for cognitive radio networks [5].

2.9 Standards and Applications Supported by CRN

Cognitive Radio Network is an improvement and advancement in the era of wireless technology. Hence there is need to throw some light in some of the standards supported by the network.

(a) Wireless Ethernet and Wi-Fi

Cognitive radio network technology supports several standards and technologies for wireless LANs like the IEEE802.11b which is presently having the widest area of coverage and deployment. There are also other standards like IEEE802.11g and IEEE802.11i, but the standard with the widest coverage is IEEE802.11b also known as Wi-Fi. They all belong to the family of wireless protocols which are collectively known as IEEE 802.11. International organizations such as IrDA creates and promotes interoperable, low cost, infrared data interconnection standards, and Home RF which is a subset of the International Telecommunication Union (ITU). IEEE802.11b transmits an unlicensed radio spectrum at 2.49Hz and also provides wireless access at 11Mbps. The media access control (MAC), and the physical layer for a wireless local area network LAN is defined by the IEEE802.11b standard. The physical layer makes use of a Direct Sequence Spread Spectrum (DSSS) that encodes each bit into a bit pattern called a chipping code. It is not a multiple access protocol because it does not support coordinated control channel access from multiple hosts. DSSS is a physical layer that spreads its energy in a signal over a wider frequency range, thus, improving the receiver's ability to recover the original transmitted bits [44].

(b) Bluetooth

This is an improvement and advancement of the existing LAN techniques but highly distinguished by its high-speed, low power, microwave wireless link technology which is designed to connect phones, laptops, personal digital assistants (PDAs) and other potable equipment that takes little or no effort from the user. The connected units or devices in Bluetooth technology do not require line of sight positioning like the infrared. All Bluetooth- enabled devices within close range instantly transfer addresses information and build small network beach among each other without user involvement [44].

(c) Wi- Max

The Wi -Max technology is a superset of Wi-Fi which is specifically designed for last-mile distribution and mobility. Its speed is proposed to be 30Mbps+. However, Wi- Max products are expensive and it is relatively a new standard and development in wireless technology. [44]

(d) Telecommunication

Telecommunication involves wireless mobile communications which are infrastructure based. A typical example is Global System for Mobile Communications (GSM). In today's mobile communication commerce and industry, the most utilized is the mobile phone. Mobile phones are based on GSM, using the technology on Time Division Multiple Access (TDMA), which accommodates a wide range of users despite geographical location and position. The GSM system uses radio infrastructures called base transceiver stations (BTS) and operates in the frequency of 900 MHz to 1.8GHz. It uses a component called subscriber identity module (SIM card) which contains an international mobile equipment identity (IMEI). The SIM stores the subscriber identity and IMEI is an international device for recognition in the mobile sphere.

The GSM mobile phone connects the user to a telephone network via the phone number, which is associated to the SIM card that keeps the address book of the user. It transmits data and information by converting the speech or voice utterances intro streams of data. When a mobile phone is switched on it automatically logs on to the network with the best

signal strength and keeps updating as it moves from one location to another via the base station using as little power, radio transmission and computing overhead as possible. This application was deployed first in the Europe in 1992 and was introduced in Africa in the late 90s and has a wide range of acceptance and coverage [45].

2.9.1 Applications Supported by CRN

The CRNs can be deployed in network-centric, distributed, ad hoc architectures, and serve the needs of both licensed and unlicensed users and applications. However, some examples of applications supported by this standard are:

(a) Robust delivery of high definition video inside home and across multiple walls.

(b) Robust coverage inside buildings and across campuses for wireless data applications such as wireless VoIP and mobile unified communications.

(c) Enhanced range for municipality, community and rural internet access without sufficient line of coverage.

(d) Enhanced coverage for smart service and remote machine-to-machine and RFID deployments such as smart grid, smart metering, transportation, industrial automation, supply chain automation, asset tracking and environmental monitoring.

(e) New interactive applications for TV broadcasters, such as weather and news updates, upcoming program previews, interactive advertisements and games and web access.

(f) Most importantly, TVWS can provide enhanced range, robustness and quality for emergency-response and public service communication networks [3].

2.10 Network Security and Privacy

The phenomenal growth of the internet and wireless communications has led to the rise in the variety of network applications and services that are pervading our lives on daily basis. The myriad of the wireless devices that enables access to the network resources on the move (anywhere, anytime) have greatly boosted the trend. Consequently, security and privacy issues have emerged in almost every aspect of the wireless and mobile computing

paradigm which cuts across wireless communication security, network denial of service, DoS attacks, secure network protocols, and mobile privacy. The inherent characteristics on mobile computing and wireless networks have posed greater challenges on its security and privacy solutions on conventional, wired networks security approaches. Therefore, a wide range of wireless and mobile network security and privacy issues have been explored and presented in a broad area. This is to throw more light into the fundamental security and privacy challenges surrounding wireless networks and the need for a rapid improvement on the design of a secured mobile wireless networks and applications.

The following are some intrusions or attacks that are common to CRN as indicated in Figure 3.4 which shows an intrusion scenario using IDRM.

(i) Denial of Access

This is an unauthorized use of the spectrum band resulting into the primary (licensed) users losing access to the network resources and services. Most times the network is being hijacked by these malicious users for selfish use and personal gains. When a cognitive radio node emits power in an unauthorized spectrum, it makes primary users to lose access and malicious entities take advantage of this nature to intrude and seize the network.

(ii) Eaves Dropping of Cognitive Messages.

Cognitive radio messages can be intercepted by a malicious user who can make use of the information to launch several other attacks on the primary users of the network or the network itself.

(iii) License User Emulation

Licensed users can be emulated by malicious users impersonating their details, camouflaging some trusted nodes, causing other nodes to join the network undetected, and sending false routing information [21]. Transmitted packets can be intercepted while on transit by malicious users, thereby having access to cognitive messages to their advantage. Malicious cognitive users can exchange or alter cognitive messages for

ulterior motives and as well change cognitive radio nodes causing interference and internal node failure which can result into network failures.

(iv) Jamming of Cognitive Radio Channels

Cognitive channels that transmit messages can also be made to jam in order to disrupt the messages passing through the network. The cognitive control channels (CCC) are made to transmit wrong messages or right messages in wrong forms. This makes the network fall short of the quality of service (QoS) assurance.

2.10.1 Fundamental Security Objectives for Cognitive Radio Networks

Security objective differ depending on the application environment. Different combinations of these features are required based on the networks configuration, service and networks policy. However, common objectives exist that provide basic security controls in cognitive radio network environments and other wireless networks due to their operation on wireless media. Cognitive radio network is a system that employs and embraces a more complex set of heterogeneous users sharing spectrum resources, and the readiness to share is encouraged using effective and efficient protocol measures. Cognitive radio automatically detects unutilized, vacant spectrum and dynamically forms suitable number of channels in order to optimize spectrum usage, increase and improve spectrum efficiency and reduce interference [18]. It is able to adapt to service environment and adjust channels bandwidth, while considering locally used traffic distribution. Cognitive radio networks (CRNs) has three aims: to innovate, improve, and maintain existing wireless communication network [20].

However, these aims cannot be realized when the security concepts are breached. Cognitive radio network security is a customizable level of security that enables any system to organize its structure and it is able to conform to requirement changes. This security system secures monitors and analyses traffic and data packets to ensure that CRNs intrusions threats or attacks are detected, and access is granted to only the right users. It enables audit trails and keeps records of previous attacks and changes to indicate, where, when, how and who made the changes [12]. These objectives basically form the fundamental principles of any network security. The goal of this research work

emphasizes mainly the intrusion detection and response model as security mechanism against all forms of CRNs intrusions or attacks to enhance security in CRNs [21].

In CRNs, reliability is achieved by applying security principles and access control measures, which involve hardware, software, applications and protocols, logical and physical policies. If specific security conditions are applied to all users of a network, information systems, and information resources, using stipulated rules, then reliability and quality of service is guaranteed. The security requirements for a reliable CRN include: availability, identification, confidentiality, integrity, authentication, authorization and non-repudiation.

(i) Availability

One of the basic objectives and aim for building a stable communication system is availability and robustness. If a network is not available, it is not usable and the objective is defeated. Security data and service profile information should be available for easy confirmations. Wireless transmission medium should always be available. The spectrum should be available for both primary and secondary users. Secondary users should not interfere or disrupt primary users by occupying the spectrum when needed. Security measures are to ensure that attacks are prevented.

(ii) Identification

This is a verification of security data and service profile information. It is a basic security objective for any communication device. It is also the process of establishing the identity of the users and other entities involved in the operations. It associates the user with a unique name. An equipment identity is assigned to all mobile devices in cellular and wireless networks called internal mobile equipment identifier (IMEI). However, tamperproof identification measure inbuilt in secondary devices is a security requirement in CRNs [20].

(iii) Confidentiality

A secured communication network such as CRN should be private and confidential for effective data and information management. This is a security requirement that ensures that only the sender and the receiver (parties and entities) involved are able to understand the communication flow. Confidentiality entails privacy and trust relationship. This means that transmission and management of data and information (communication) among users and devices in cognitive radio network must be confidential and the entities involved must ensure a mutual agreement of trust to guarantee quality of service.

(iv) Integrity

Data packets can be intercepted or modified in transit by attackers for malicious use. Therefore, a secured communication in cognitive radio network requires integrity in order to establish effective transmission of data packets and management of data and information to achieve quality of service. Integrity ensures that data and information are not changed or modified in transit. Any change or modification must be done by the explicit consent of the entities involved. The receiving end or entity must be assured that the data packets or information received or is receiving is exactly what was transmitted from the transmitting end. Therefore, this objective ensures privacy of authorized user data and control information in cognitive radio network for effective data and information management.

(vi) Access Control

This restricts network's resources to authorized users or devices only. It ensures that every user or device in a network has the explicit right to access the resources requested for and also the privileges to perform certain tasks in a network. This objective forms the basis for validating any security mechanism.

2.11 Chapter Summary

This chapter consists of a survey of existing work in cognitive radio networks in literature. It also explains the key terms used in the research project, and the components

of cognitive radio network. It explained the intrusion detection system (IDS), followed by the features of cognitive radio network capability, CRN protocol layers, standards, and applications supported by CRN, network security and privacy issues, and then the fundamental security objectives for CRNs.

CHAPTER THREE
INTRUSION DETECTION AND RESPONSE MODEL

3.1 Chapter Overview

This chapter focuses on the requirement analysis and development of the intrusion detection and response model (IDRM) to enhance security in CRNs. The chapter starts by introducing the current state-of-the-art on security in CRNs followed by the vulnerabilities and attacks in CRNs. This aspect is introduced in order to create a distinction between what exists and what this research intends to advance. More so, it provides a response to the research questions 1, 2, and 3 and the corresponding research objectives. The IDRM security requirements and the IDRM developed in this research work are also presented.

3.2 State-of-the-art on Security in Cognitive Radio Networks.

The main objective here is to analyze the existing work on security in cognitive radio networks, so as to create the distinction on what previously existed and what is presently achieved in this research project. Security in cognitive radio networks is a major challenge in the deployment of this new technology that has revolutionized our view of opportunities in wireless communication to a great extent. Attackers have taken advantage of the free allocation of the spectrum band to replicate attacks to cognitive radio networks on daily basis. Therefore, researchers have not relented in finding security mechanisms that are capable of providing adequate security to cognitive radio networks and ward off the intruders. This section of the research project presents some of the current or existing endeavors on security in cognitive radio networks as in Table 3.1. The table consists of three columns, where the first column contains the list of researchers, the second column contains the research contributions and the main ideas, while the third column contains the research achievements.

Table 3:1 Analysis of existing research on security in cognitive radio networks

Researchers	Research Contributions/ Main Idea	Research Achievements
Zhang et al [17, 18]	Developed a distributed and collaborative architecture for detecting misrouting packet dropping using anomaly detection technique.	The security mechanism verifies all data packets to identify attacks in all mobile networks.
P. O. Albers [19]	Developed a distributed and collaborative architecture using misuse and anomaly detection technique.	The security mechanism identifies attacks in distributed wireless networks
B. Sun et al [35]	Developed a distributed and collaborative architecture using anomaly detection technique.	The security mechanism identifies attacks in distributed wireless networks.
Jin et al [50]	Applied the finding characteristics of wireless environment in mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing.	The security mechanism is for detecting attacks in dynamic spectrum access.
Jin et al [51]	Used analytical models for the received power for attack detection	The security mechanism is for detecting primary user emulation attacks in dynamic spectrum access.
Cheng et al [10]	Applied a separate sensor networks for detecting primary user emulation attacks such that the primary users are not responsible for detections.	The security mechanism is for defense against primary user emulation attacks in cognitive radio networks.
Liu et al [52]	Used novel physical layer authentication technique, light weight authentication technique and light weight authentication protocol in detecting attacks and intrusions.	Thee security mechanism is authenticating primary user signals in cognitive radio networks via integrated cryptographic and wireless link signatures.
Chen et al [53]	Considered attackers with various variable transmission powers and proposed a detection method that can be used regardless of the type of sensing.	The security mechanism modeled primary user emulation attacks and its defense in cognitive radio networks.
Mathur et al [54]	Applied a light weight public key cryptography mechanism between primary users and secondary users.	The security mechanism used digital signatures for centralized dynamic spectrum access networks.
Wang et al [55]	Developed a two typed robust detection scheme that combines the suspicious level and the trustworthiness of the users	The security mechanism used an attack proof collaborative sensing technique for cognitive radio systems
Li et al [56]	Considered two attack strategies that depend on whether the attackers know the reports or information sent by other user.	This security mechanism is catching attacks for collaborative spectrum sensing in cognitive radio networks using an abnormality detection approach.
Zhu et al [57]	Proposed two algorithms for attack detection with higher performance	This security mechanism enhanced robust cooperative spectrum sensing in cognitive radio.

Consequently, it has become evident from the analysis of findings specified in the Table 3.1 that an appropriate security infrastructure that is compatible to the self-characteristics of cognitive radio networks, providing maximum security and quality of service, is still far-fetched. Therefore, in this research project an Intrusion Detection and Response

Model (IDRM) that is capable of enhancing security in cognitive radio networks is developed.

3.3 Vulnerabilities and Attacks in Cognitive Radio Networks.

In order to achieve the main goal of this research the second objective is to investigate some of the vulnerabilities and attacks which are associated with cognitive radio networks. Reported in Table 3.2 is a summative investigation of the various types of attacks, security requirement and the specified CRN functionality affected by the attack.

Table 3.2: Vulnerabilities and Attacks associated with CRN [46, 47, 48, 49, 50].

Attack Description	Security Requirement	CRN Functionality Affected
Jamming of cognitive radio channels.	Robustness and, protection of integrity.	Spectrum sensing and, spectrum sharing.
Denial of service.	Compliance to the networks regulatory framework (service, security policy).	Spectrum sharing
Primary user emulation.	Verification of identities and, accountabilities.	Spectrum sensing and, spectrum mobility.
Eavesdropping of cognitive messages.	Protection of message or data confidentiality	Spectrum sensing and spectrum sharing.
Disruption to MAC or the cognitive engine of the cognitive radio network.	Verification of identities, controlled access to resources, protection of system integrity.	Resource management and, data management.
Saturation of the cognitive channel.	Robustness, protection of system integrity.	Spectrum sharing and, spectrum sensing.
Selfish use of the spectrum band by unauthorized users.	Compliance to the networks regulatory framework (service, security policy).	Spectrum sharing and, spectrum mobility.
Hidden node problem.	Compliance to the networks regulatory framework (service, security policy).	Spectrum sensing, spectrum sharing, and spectrum mobility.
Masquerading of cognitive radio node.	Verification of identities, accountability and, controlled access to resources.	Spectrum sensing and, spectrum sharing.
Malicious alteration of CR node.	Protection of systems integrity, compliance to the networks regulatory framework (service, security policy).	Spectrum management, spectrum sharing and, spectrum mobility.
Malicious alteration of cognitive radio messages.	Protection of data integrity, verification of identity.	Spectrum sensing and, spectrum sharing.

Table 3.2 shows a summary of the types of attacks, its associated security measures and the CRN functionality that is affected. This investigation is imperative as it enable us to

understand: (i) the types of attacks that are specific to CRN aside the attacks which are common to other traditional and conventional wireless networks which IDRM is designed in this research project to address: (ii) the various security requirements for each of the attacks, and (iii) to construct a suitable intrusion detection scenario based on some of the attacks.

3.4 CRN Service and Security Policy for IDRM

Cognitive radio network security policy is not stated as part of this research objective, but because the IDRM employs the specification-based intrusion detection method using systrace - a computer security utility which limits or restricts an application's access by enforcing networks security and service policy for all system calls - it cannot be left out. The security policy is formulated based on the distinctive features and characteristics that best describe the CR network. This security reflects the various security requirements and descriptions specified in this research project and also provide the network's needs. The CRN-based company or organization implements this policy in order to be guarded against unauthorized and uncontrolled wireless malicious hackers that are bent on network intrusion. The use of this policy enables the IDRM to effectively detect deviations and noncompliance to the policy as intrusions. It also provides the CRN-based company or organization with strong security protection so as to enjoy the economic dividends brought about by CRN.

3.4.1 Purpose of the Policy

The policy establishes standards that must be met when a client's wireless communication equipment or device is connected to CR networks. The policy prohibits access to CR networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by the CRN Information Security (CRNIS) are approved for connectivity to CR networks, otherwise access is disallowed or denied. This is due to the type of specification-based intrusion detection method employed by IDRM which restricts user's access to the network by enforcing the networks access and security policy on all system calls.

3.4.2 Scope of the Policy

The policy embraces all wireless data communication devices such as personal computers (PCs), cellular phones, personal digital assistance (PDAs), etc.), connected to any of CR internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to CR networks do not fall under the purview of this policy.

3.4.3 The Policy

This constitutes the body of the security policy for cognitive radio network and it includes: approved equipment, monitoring of uncontrolled wireless devices, authentication of wireless clients, encryption, access control policies, remote wireless access, client security standards and wireless guest access.

(a) Approved Equipment

All wireless LAN access must use corporate-approved products and security configurations.

(b) Monitoring of uncontrolled wireless devices

All uncontrolled wireless devices connected to the network must be monitored and controlled using the conditions outlined below.

(i) All cognitive radio networks' locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect, classify, and disrupt communication with unapproved wireless access points.

(ii) All company locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect the presence of wireless devices forming a connection between the network and other wireless networks. This would include laptops that are serving as a bridge between wired and wireless networks.

(iii) In company locations where wireless LAN access has been deployed, wireless intrusion detection and response system will also be deployed to monitor attacks against

the wireless network. The IDRM shall be integrated with the wireless LAN access system.

(c) Authentication of wireless clients

Authentication of all wireless clients and users is necessary to ensure that all identities are verified and validated and the clients are who they claim to be. Therefore;

(i) All access to cognitive radio networks must be authenticated.

(ii) The Organization's existing strong password policy must be followed for access to the cognitive radio networks.

(iii) The strongest form of wireless authentication permitted by the client device must be used. For the majority of devices and operating systems, Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access Version2 (WPA2) with 802.1x or Extensible Authentication Protocol (EAP), Protected Extensible Protocol (PEAP) must be used. WPA2 is preferred wherever possible.

(iv) Where 802.1x authentications are used, mutual authentication must be performed. Client devices must verify and validate that digital certificates presented by the authentication server are trusted and valid. Under no circumstances should clients disable validation of server certificates and blindly trust any certificate presented. EAP methods that do not support certificate-based mutual authentication may not be used.

(v) EAP methods that exchange authentication credentials outside of encrypted tunnels may not be used. These methods include Light Weight Extensible Authentication Protocol (LEAP).

(vi) When legacy devices that do not support WPA or WPA2 must be used on a wireless network, they will be isolated from all other wireless devices and will be restricted to the minimum required network access. Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.

(vii) Any organization or company user with an account in an organization or company user database shall be able to authenticate at any CRNs location where wireless access is present.

(d) Encryption

Encryption of all communication in and out of the network is very necessary because intruders cannot make use of data when it is encrypted. Therefore:

(i) All wireless communication between Cognitive Radio Networks devices and Cognitive Radio Networks must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement.

(ii) The strongest form of wireless encryption permitted by the client device must be used for the majority of devices and operating systems.

(iii) Client devices that do not support WPA or WPA2 should be secured using Virtual Private Network (VPN) technology.

(iv) The use of Wired Equivalent Privacy (WEP) requires a waiver from CRN Information Security. Client devices that require the use of WEP must be isolated from all other wireless devices and will be restricted to the minimum required network access.

(v) Violations of the configured rules, indicating that an intrusion has taken place, must cause the device to be immediately disconnected and blocked from the network.

(e) Access Control Policies

Access to the resources made available by the CR network must be controlled using the policies outlined below.

(i) Access to corporate CR Network resources through wireless networks should be restricted based on the business role of the user. Unnecessary protocols should be blocked, as well as access to segments of the network which the user has no need to communicate.

(ii) Access Control Enforcement (ACE) shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security (IDS)."

(iii) The access control system must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.

(iv) Access control rules must use Specification-based control as the underlying analysis mechanism.

(f) Remote Wireless Access

The CR network should not be weakened because users are not at the corporate stations. It must be uniform despite the users' access point to the network. Therefore;

(i) Telecommuting employees working from remote locations must be provided with the same wireless standards supported in corporate offices.

(ii) Employees should be discouraged from connecting networks computers through consumer type wireless equipment while at home in lieu of company-provided equipment.

(g) Client Security Standards

Where supported by the client operating system, the wireless network will perform checks for minimum client security standards (client integrity checking) before granting access to the Cognitive Radio Network. Specifically:

(i) All wireless clients must run CRN approved anti-virus software that has been updated and maintained in accordance with the Network's anti-virus software policy.

(ii) All wireless clients must run host-based firewall software in accordance with the CRNs host security policy.

(iii) All wireless clients must have security-related operating system patches applied that have been deemed "critical" in accordance with the CRNs host security policy.

(iv) All wireless clients must be installed with company-standard wireless driver software.

(v) Clients not conforming to the approved minimum security standards will be placed into a quarantine condition and automatically remediated.

(vi) Client operating systems that do not support client integrity checking will be given restricted access to the network according to networks business requirements.

(h) Wireless Guest Access

Wireless guest access will be available at all facilities where wireless access has been deployed, but controlled by the following regulations:

(i) All wireless guest access will be authenticated through a web-based authentication system.

(ii) A single username/password combination will be assigned for all guest access. The password for guest access shall be changed monthly and distributed to local facility managers.

(iii) Wireless guest access is bandwidth limited to 2Mb/s per user.

The network security policy specified above is important because of the distributed and dynamic nature of cognitive radio networks and the intrusion detection method employed by the model designed in this work. Therefore, for effective deployment and implementation of the designed model, the network security policy must be specified and enforced on all network connectivity.

However, the requirement analysis of the corresponding security requirements for developing the IDRM system is presented in section 3.5 and 3.6.

3.5 IDRM Requirement Analysis

The design and development of an intrusion detection and response model that enhances the security level in CRN is the fundamental aim of this research project. It is therefore,

necessary to firstly specify the basic requirement of the designed model before the actual implementation. However, the requirement for the implementation of the IDRM consists of monitoring and analysis, features selection, automated response, warning and storing. This requirement provides IDRM with the capabilities that enable it to enhance security in cognitive radio networks.

When data packets are transmitted into the CR network, it is checked based on the network security policy. The network is configured using a detailed security policy that controls both the access to the network resources, incoming and outgoing data packets. This enables it to monitor, examine and analyse the traffic flow against any form of intrusions.

Apparently, the IDRM design, implementation, and deployment are based on the intrusion signature and security policy based method for detecting intrusions. The network security policy is enforced on all incoming and outgoing data packets. The database for intrusion specification database is accessed to determine the pattern of intrusion and the predefined profiles or definitions of intrusion activities stored in the database for each protocol state in the entire CRN layer in order to identify deviations. The point of interception by the IDRM ensures that all packets from the client host and each of the network hosts are verified and validated to either be allowed or disallowed respectively.

Consequently, the IDRM works effectively and efficiently in collaboration with other security mechanisms which provide preventive measures such as authentication, authorization and access controls like firewalls. Each of these access servers verifies all clients devices (users) connected to the CR network using its verification essentials based on CRN configuration and security policy. If intruders or attackers bypass these "check points" launching various intrusions, the IDRM is then on monitoring and intercepts and rescues the situation. It ensures that all data packets transmitted in the entire network layers are properly examined to detect the specific intrusion, and responds adequately to protect the entire network and put the system back to normal.

(i) Monitoring and Analysis

Once a client or any host system or network connects to the CRN network, the IDRM traffic collector is at alert providing a comprehensive monitoring functionality required for an effective and efficient security infrastructure capable of enhancing security in cognitive radio networks. This it achieves by monitoring all traffic across the CR networks and pulling all data and information transmitted at different levels across the network to be properly examined and analyzed for accurate intrusion detection.

The analysis engine of the IDRM provides a comprehensive accessing, analysis and detection of CRN intrusions and vulnerabilities. The variable or components for assessment are co-located with or integrated into the sensors or coordinators of the IDRM. These components translate, analyze, and correlate all traffic, data and information supplied to it by the traffic collector to identify suspicious activity and matching patterns of vulnerabilities and exploitations. The analysis capability is able to operate on historical data and operate in real or near-real time to assess the current state of the CR network. This capability is available at both levels to provide a comprehensive and advanced security in cognitive radio networks.

(ii) Features Collection

The IDRM traffic collector collects features of packets and vulnerability data for intrusion in both real time and non-real time. It collects all suspicious traffic and information that describes or characterizes the traffic and identifies various network components, connections or associations. Through this it is able to detect and identify intrusions or attacks specific to a designated network area or system, and detect denial of service attacks to include service overloads, broadcast storms, and message flooding, IP address spoofing and others. It automatically keeps records of events and incidents within the network since CRN is an intelligent and distributed network with self-automation characteristics. By monitoring networks and hosts and analysis of transmitted data packets, the features such as content, context, packet header are selected for intrusion detection on multiple platforms hosts, switches, routers and, others.

(iii) Automated Response

The IDRM has the capabilities to automatically respond to identified intrusions or attacks and vulnerabilities either by shutting down the port, dropping the packets or disconnecting the device from the network. These capabilities are necessary to enable the CRN recover from attacks, reconstitute resources to ward off intruders or ameliorate vulnerabilities, and restore disabled network capabilities. However, these capabilities also enable the IDRM to participate in enforcing the network security policy on all the network's subordinates.

Responses to detected intrusions include the ability to disallow the intruders or attackers access to the network. The type of response depends on the type of intrusion. The IDRM is in control of any connection or association, such as connectionless traffic between two systems using the user datagram protocol [UDP]). It should be able to terminate connections and effectively disallow access to a network or host whenever a malicious act is suspected. Denial of service attacks such as broadcast storming, message flooding, and service overloading limit effectiveness and quality of service, hence, IDRM is able to react and respond to them effectively. Response to intrusions includes capability to take automated and predetermined actions.

In general, IDRM sensors are able to turn themselves off and on in response to predefined conditions. IDRM has configurable features or capabilities that: (1) enables proper response to intrusions, vulnerabilities and suspicious events; (2) track and log activities across all ports and services of an internet protocol (IP) address identified as connected or associated with any intrusions or malicious activity; (3) automatically react with predefined defensive techniques and procedures for recovery and reconstitution.

The IDRM can access any port or service associated with any detected intrusion, vulnerability or identified suspicious activity for a configurable period of time. It can isolate an IP address with respect to continued activity once the IP address is identified as being connected or associated with suspicious activity. Any specific response taken for each intrusion detected can be logged by the IDRM.

(iv) Warning

The IDRM provides real-time warning for suspected events and detected intrusions. This is displayed to a user console and is configurable as visual. The warning provided by the IDRM is easy to understand and is implemented in a manner that avoids operator and system overloading. The IDRM has the capability to send warnings to appropriate organizations or devices or owners of the systems used for the attack.

(v) Storing

The IDRM has the ability to collect information about verified intrusions and vulnerabilities and send to the central database for analysis and long-term storage. It stores in archival storage at the centralized database to enable certain kinds of analysis such as to discover whether a particular intrusion/attack that is being investigated has been seen at any network segment or devices connected to the network or host systems for a review of sequence of networking events involved in an intrusion.

3.6 Use Case

This section of the requirement analysis provides a description of the intrusion detection and response model using use case. It shows how information and data packets in cognitive radio network are protected and secured using IDRM as an access control measure. Intrusion Detection and Response Model is a security mechanism that monitors the entire network to detect unwanted, unauthorized malicious use and users of the CR networks. It is also capable of initiating a quick response once a malicious act or an unauthorized activity is taking or has taken place within and outside the CR networked systems. It is configured to automatically respond to intrusions and also to notify network security analysts (NSAs) and management directly of trouble via e-mail or pagers.

The techniques used to achieve IDRM responsibility are: intrusion signature–based and service and security policy misuse. The server uses these processes to determine the data packets or traffic that should be allowed or disallowed. Some of the components of the use case for IDRM are network connections, data collection, feature selection, analysis, allow, and disallow data traffic.

3.6.1 Use Case Diagram Describing IDRM

The use case diagram describing IDRM is shown in Figure 3.1. IDRM monitors for signs of intrusive activity. It is designed to generate automate response whenever an intrusion is detected. This response mechanism is based on intrusion detection technique or method applied in this research project. To implement the response mechanism, the IDRM needs to monitor at specific locations in the host base and the layers of the network base. IDRM is a hybrid model and so operates as both the host based and the network based. It combines both approaches to maximize its protection capability.

The IDRM use case diagram provides a detailed explanation of its detection process. It is separated into five components such as: network connectivity; data collection and feature selection; monitoring and analysis; intrusion detection, and response, which consists of allow and disallow access. This forms the active detection process.

The client host device (user access) is usually an untrusted system or network and data packets are transmitted through an external router to the network server. Consequently, connectivity is established between the CRN server and the client host. The IDRM is steadily tuned on to monitor and analyze data packets transmitted in and out of the network. The data or information captured is collected by the traffic collector; the features are selected for the IDRM analysis engine for intrusion detection.

Once the data is confirmed to be any form of intrusion, the data traffic is disallowed and quick automated responses are sent to the intruders' device and all relevant information about the intrusion is stored in the intrusion detection database for further analysis by the networks security administrators (NSAs). The automated responses are based on the IDRM configuration which includes, access allowed, access disallowed, IDRM drop the packet, shut down the port.

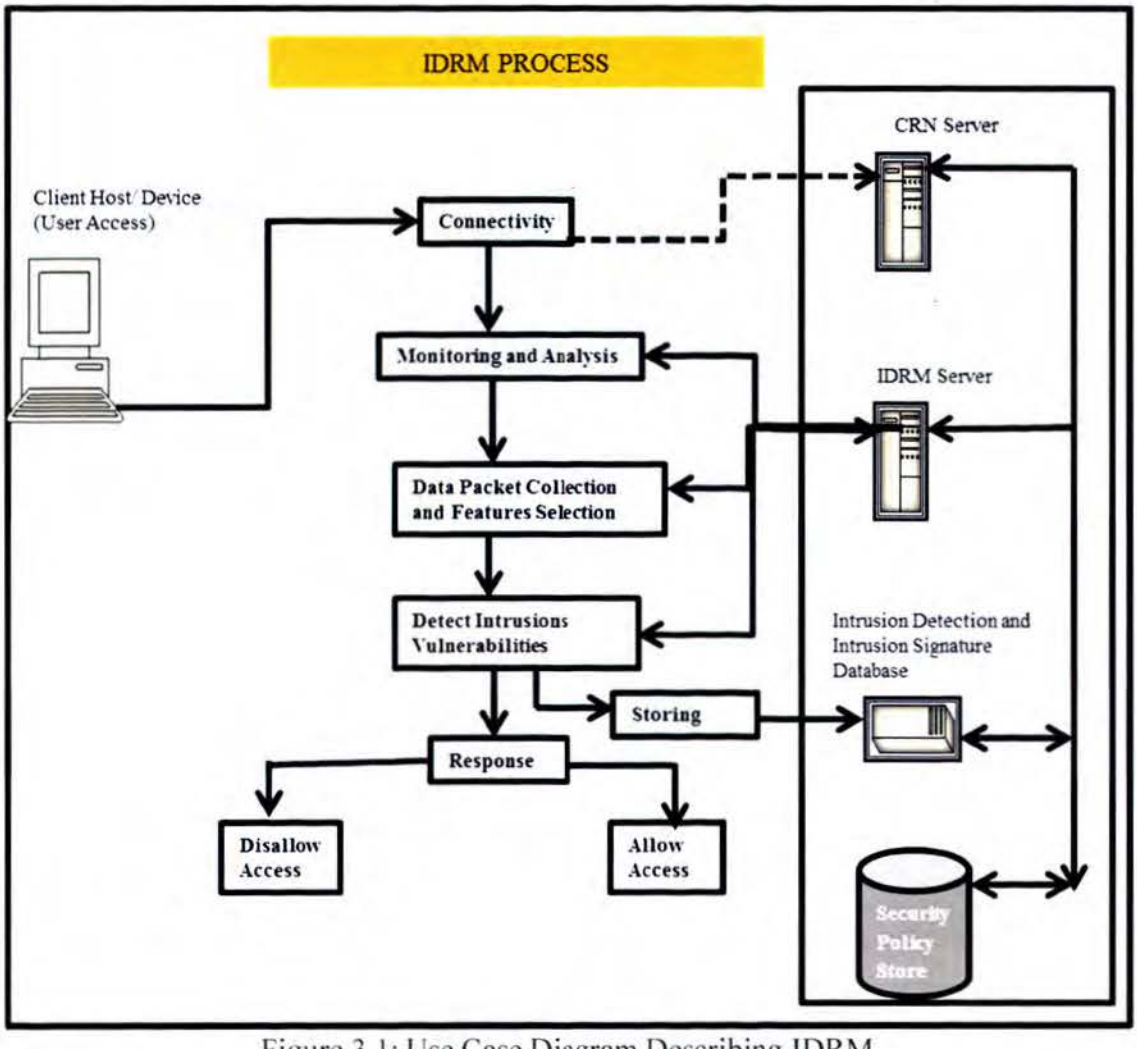


Figure 3.1: Use Case Diagram Describing IDRM

3.6.2 Use Case Analysis

The intrusion detection and response model is further analyzed using use case tables (Table 3.3 to 3.7). The description process employed in the use case has two phases, which are intrusion detection and automated responses (which constitute the main aim of this research work). The intrusion detection phase consists of the network connection sequence, the data collection sequence, features selection sequence, and the analysis which results into intrusion detection. However, the detection of intrusion is based on the service and security policy and the intrusion pattern stored in the database, while the response phase consists of the several automated responses appropriate for the intrusion such as access allowed, access disallowed and warning. The rows contain the use case

name, the participating actor, the entry condition, the flow of events, and the exit condition while the columns contains the explanations of the rows respectively. The details are shown in Tables 3.3 - 3.7.

(i) Network Connection

Table 3.3: Connection Sequence

Use Case Name	Network Connection.
Participating Actor	Initiated by Client Host
Entry Condition	The client hosts logs into the CRN server.
Flow of Events	Transmits data and packets to the CRN server
Exit Condition	IDRM analysis and detection process begins.

(ii) Data collection and Analysis

Table 3.4: Data Collection and Analysis Sequence

Use case Name	Data Collection and Analysis
Participating Actor	Initiated by CRN server
Entry condition	Transmitted packets and real time data in the host system is collected by the IDRM traffic collector and passed over to IDRM analysis engine.
Flow of Events	IDRM analysis engine intercepts and analyzes the data and transmitted packets. The Networks Security Policy Enforcement Agent (NSPEA) and Networks Security Policy Decision Agent– checks to verify the user security data and service profile based on the network configuration and network security policy (NSP).
Exit condition	Details such as disk usage, system process, call stack etc. are logged.

(iii) Features Selection

Table 3.5: Features Selection Sequence

Use case Name	Features Selection
Participating Actor	Initiated by IDRM
Entry Condition	The Internet Protocol (IP) address of the source and target system, protocol type, header length and size for examinations could be studied for possible intrusion
Flow of Events	IDRM takes a subset of the available data packet in network to be studied and analysed for possible intrusions.
Exit Condition	If any forms of intrusions are suspected, IDRM automatically suspends the network flow until proper analysis and verifications are made.

(iv) Intrusion Detection

Table 3.6: Intrusion Detection Sequence

Use Case Name	Intrusion Detection
Participating Actor	Initiated IDRM.
Entry Condition	IDRM inspects the result from the SPEA and SPDA based on the service and security policy and, intrusion pattern predefined.
Flow of Event	The data packets are linked to the database of the network where the incoming traffic is checked against pre-defined intrusion signature or pattern and the security policy and, compares predetermined profiles of definitions of intrusion activities for each protocol state against observed events to identify deviations.
Exit condition	A new window opens. Cognitive Radio Network Policy is accessed for approved conditions for allowed and disallowed access. IDRM automatically generates and sends a quick response. The intrusion detection information is stored in the intrusion detection database for further investigations by the NSA.

(v) Automated Response

Table 3.7: Automated Response Sequence

Use Case Name	Allow or Disallow Access, Drop the Packets, Shut down the port, Intruders Forbidden
Participating Actor	Initiated by IDRM.
Entry condition	IDRM automatically generates a quick response based on the detected intrusion during the analysis phase.
Flow of Events	IDRM stores the revenant information about the intrusion detected under its radar and decides to disallow access (network flow) and automatically drops the packets or shut down the ports.
Exist of Condition	The network flow or connectivity suspended, a further response in form of warning is also sent to the devices or company's whose devices are used for such intrusions or attacks.

3.7 IDRM Algorithm

The IDRM is designed and configured to monitor and analyse the activities of the CR Network as displayed in Figure 3.2.

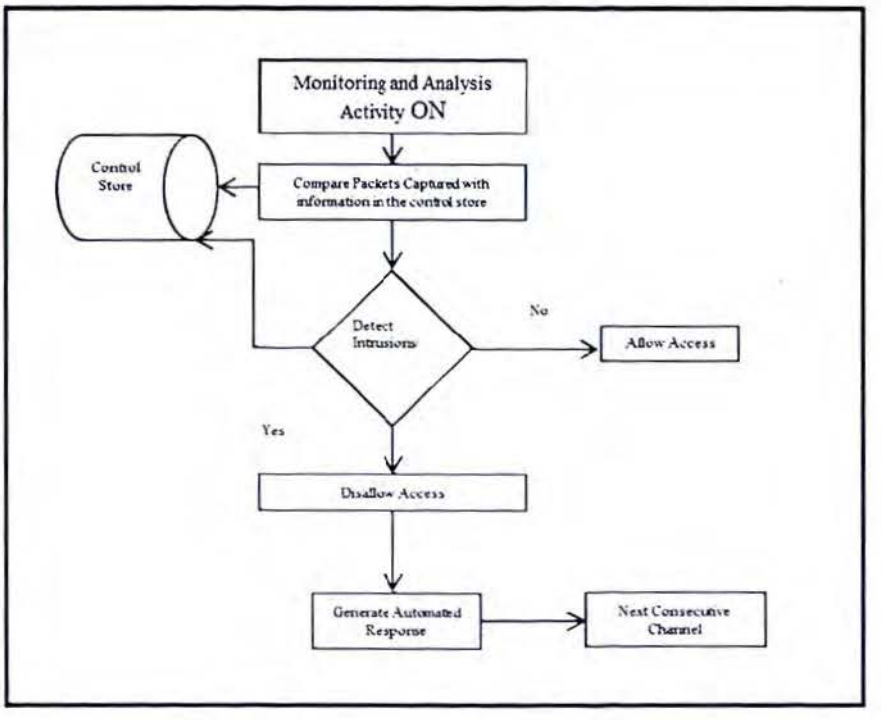


Figure 3.2: IDRM Algorithm

IDRM acts as a packet monitoring and analyser to monitor and analyse the nodes in connection and communication with each other within the network. It monitors the coordinators and the routers in real time. The packets that are captured are compared to the database or knowledge base of the intrusion specification, service and security policy that are previously configured on the bases of intrusions which are common to the network.

Fundamentally, the IDRM is set up to detect or discover framed packets that have formats not compatible with the networks configuration. The IDRM which is steadily tuned on starts monitoring and analysing the network traffic immediately the network connection is formed. It is connected to all the required devices or appliances (network layers, routers, coordinators, nodes, protocols) for comprehensive checking. Transmitted packets are captured and compared with the information in the control store (access, service and security policy,) and the networks CRN database. The corresponding intrusions detected are stored in the intrusion detection database. To react to any intrusion detected or discovered, the IDRM is required to generate an automated response suitable

for the attack and a form of warning to the intruder and stores the intrusion pattern into the intrusion detection database before moving to the next consecutive channel. If the IDRM detects an ID conflict, it automatically disables itself from the coordinators and performs an active scan to select the new appropriate ID. As soon as this happens, a channel message from the channel master is sent across, and promptly the operating channel is changed to the new ID and the monitoring activity is tuned on for further checking.

3.8 Intrusion Detection and Response Model (IDRM)

Figure 3.1 is an IDRM design as a security mechanism to enhance security in CRN by providing secure communication, enabling efficient resource allocation, effective spectrum usage, and access control to the limited and scarce resources. The IDRM that was designed achieved those characteristics by identifying computing or network activities that are considered as intrusions, malicious, or unauthorized. It is configured to properly scrutinize all packets at different protocol layers of the network such as; physical layer, link layer, network layer and transport layer due to accessing the spectrum dynamically.

The IDRM design shows the layout of the model and its associated components. The IDRM operates as a network-based model and provides maximum security to enhance the networks productivity and quality of service. The IDRM is designed based on three major components which are data and information source; monitoring, analysis detection; followed by the response mechanism. The operation of the model will be described according to the various components that make up the model.

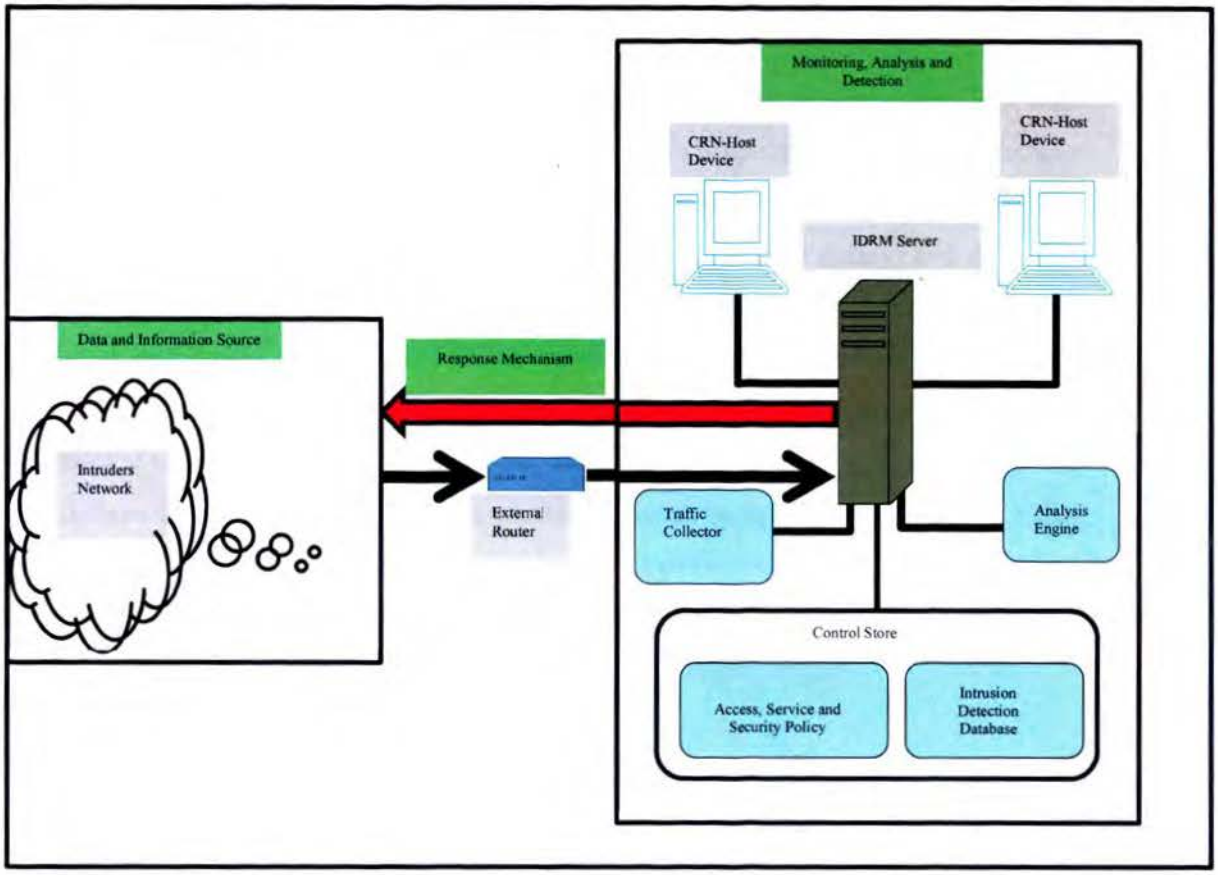


Figure 3.3: Intrusion Detection and Response Model (IDRM)

(i) Data and Information Source

Data and information source contains the intruders' network, consisting of all wireless and mobile devices (user access) which usually request for access or connection to the CRN network. The information sources are divided into three categories: (i) input data accumulated from individual systems (host based); (ii) input data originated from the network (network based); and (iii) data produced from other sources. However, the IDRM evaluates the operating system audit trail as its significant data source for all network layers (application, network, transport, link, physical).

(ii) Monitoring, Analysis and Detection

Monitoring, analysis and detection contain two major components which are CRN host devices and the IDRM server. Host devices consist of computers and other appliances connected to network, while the IDRM server consists of some logical components such as: traffic collector, analysis engine, access, service and security policy, and intrusion detection database. Generally, the art of monitoring, analysis and detection is the core activity of our IDRM. The IDRM is configured based on the network policy using 'systrace' - a computer security utility which limits an application's access to the system by enforcing networks access policy (service and security policy) for all system calls. By this method we determine whether a particular event is an intrusion or not. This monitoring, analysis and detection component consists of two sub components, which are IDRM Server and CRN Host Devices. The IDRM sever is made up of some logical components such as: (a) the traffic collector and (b) the analysis engine.

(a) Traffic Collector

This component of the IDRM is designed to pull traffic from the network. It collects information or activity for the IDRM to examine. This information or activities could be log files, audit logs, or incoming and outgoing traffic on a specific system. Because IDRM is network-based, the traffic collector (component) copies traffic outside the network link. This component behaves like a network traffic sniffer where every packet transmitted along its duty path of the network is to be properly examined.

(b) Analysis Engine

This component examines the network traffic that has been collected by the traffic collector. This is done by the analyser from the analysis engine. It is regarded as the most important component of the IDRM due to its responsibility for analysis and detection. It is often referred to as the brain of the IDRM. It consists of the security policy enforcement agent (SPEA) and the security policy decision agent (SPDA). The SPEA ensures connection admission control and handoff by enforcing the respective designed policies on the subjects (network users) while, the result from that component is sent to

the SPDP for implementation via SPEA based on the stipulated policy. Then a confirmation message is sent to the client via the security policy retrieval agent (SPRA). This way, the analysis engine decides the activity, communication or transmission that is allowed or disallowed. It is a decision or pattern matching mechanism. It compares the traffic and information supplied to it by the traffic collector against the networks access policy (service and security policy) and known intrusion specification (patterns) stored in the intrusions detection database. If the activity matches any known pattern, or misuse of the security policy is detected, it reacts to it as an intrusion by generating any of the automated responses based on the intrusion and gives a warning. This examination of traffic is done as quickly as possible to enable IDRM react to intrusions in real time and move to the next consecutive channel.

(c) Control Store

The control database store consists of access, service and security policy, and intrusion detection database. The analyser from the analysis engine collects relevant information pertaining to an intrusion besides the main function of identifying intrusion within the network layers. It also collects the supporting evidence and traces of the intrusions and stores them in the intrusion detection database. The networks database stores all user identity details and all normal user behaviour based on the management access, service and security policy. This enables detection of deviations as intrusions. In addition, data packets coming into the system from the five different layers of the network (application layer, transport layer, network layer, link layer and physical layer) are assembled to form complete transmission control protocol (TCP) and protocol data unit (PDU) to be analysed to check intrusions. All intrusions detected or discovered by the IDRM are duly reacted to via the response mechanism.

(iii) Response Mechanism

After analysis is done and the IDRM detects intrusions, it immediately disallows access and reacts to them by sending appropriate automated responses to the intruder's devices, such as drop the packets, shut down the port, coupled with a warning. All information

about the intrusions is stored in the intrusion detection database, also referred to as the attack signature database.

Because the spectrum is accessed dynamically, IDRM is designed and configured to influence every protocol layer. The IDRM is a network-based model therefore, it resides on computer or appliance connected to a specified segment of the network. It can also be installed at specific places in the network where it can watch traffic going into and out of particular network segment. It looks for intrusion patterns as well as deviations from service and security policy when analysing or examining packets transmitted over the network.

The primary idea of IDRM is to detect CRN intrusions while allowing genuine and authorized user access. The entire network security is identified with the network traffic by classifying the allowed and disallowed traffic.

In summary, any packet transmitted from an intruder's network to any of the CRN host devices must pass through the IDRM server engine via the external router which serves as the request messenger. This is first analysed by the IDRM that monitors the entire network in order to detect intrusions or attacks that were not handled by other security mechanisms in place (the first line of defence), and also provides quick automated responses without any human intervention. This automated response is generated by the IDRM once an intrusion is detected via the response mechanism which in turn stops it from getting to the CRN host device that is the target of the intrusion. Information that is useful to track new attacks is also provided.

The intrusion detection is based on the network configurations levels such as detection level and response level which are in connection with the network policy outlined in section 3.8.3. The scenario for intrusion detection using the designed IDRM is shown in Figure 3.4 while the algorithm and the use case diagram that further describe the IDRM are shown in Figures 3.2 and 3.1, respectively. The network IDRM security system is configured and implemented based on specification-based technique (network services and security network policy) using systrace - a computer security utility which limits or restricts an application's access by enforcing network security and service policy for all

system calls. Therefore, intrusion detection using IDRM is based on the information recorded in the attack or intrusion specification database. Intrusion detection database consists of the service and security policy specified by the cognitive radio network and also relevant information on the detected intrusions. Thus, attackers are restricted from invading the network for fear of their identity being revealed.

CRN is a distributed intelligent and dynamic network such that its IDRM is also distributed in its configuration to cover a large network area to provide an advanced network monitoring, incident analysis, incident response and instance attack data This enables the network security analysts (NSAs) to have broader view of the occurrences in the entire network per time and identify new intrusion patterns from the record of intrusion detection database. This enables further investigations on the detected intrusions. The implementation of the IDRM is reported in chapter 4.

3.8.1 IDRM UML Sequence

The IDRM UML diagram in Figure 3.4 describes the sequence of activities of the IDRM. It shows the operations of its sub components indicating the request and communication (challenge response) protocols.

When the client sends a network or resource request it passes through the air frequency bandwidth because of its wireless nature. The request is delivered to the traffic collector by the network resource broker (NRB) and handed over to the analysis engine which consists of the SPEA (security policy enforcement agent) and SPDA (security policy decision agent).

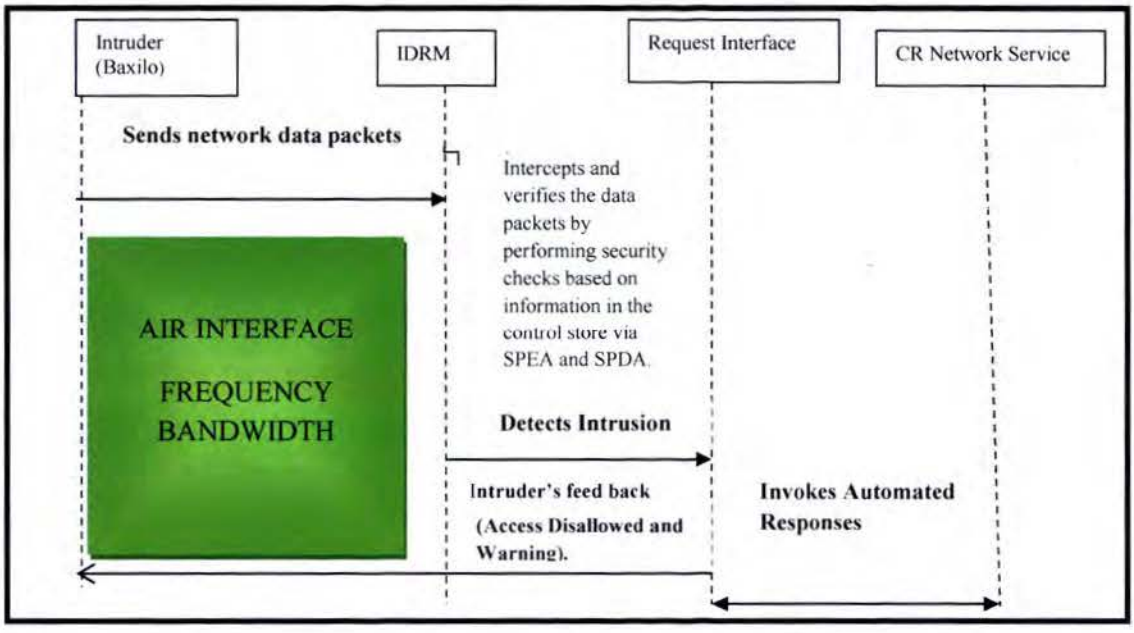


Figure 3.4 IDRM UML Sequence Diagram

The SPEA component of the IDRM analysis engine performs the verification activities based on the network service and security policy (NSSP). The message is then validated in line with the SPDA decision and the network service is invoked. The client is given feedback via the SPEA. The access is disallowed if an intrusion is detected or allowed if otherwise depending on the verification outcome.

3.9 Scenario for Intrusions Detection using IDRM

In Figure 3.5 is a scenario that describes how IDRM reacts to the various intrusions (vulnerabilities and attacks) identified in Table 3.2 as types of attacks in CRNs.

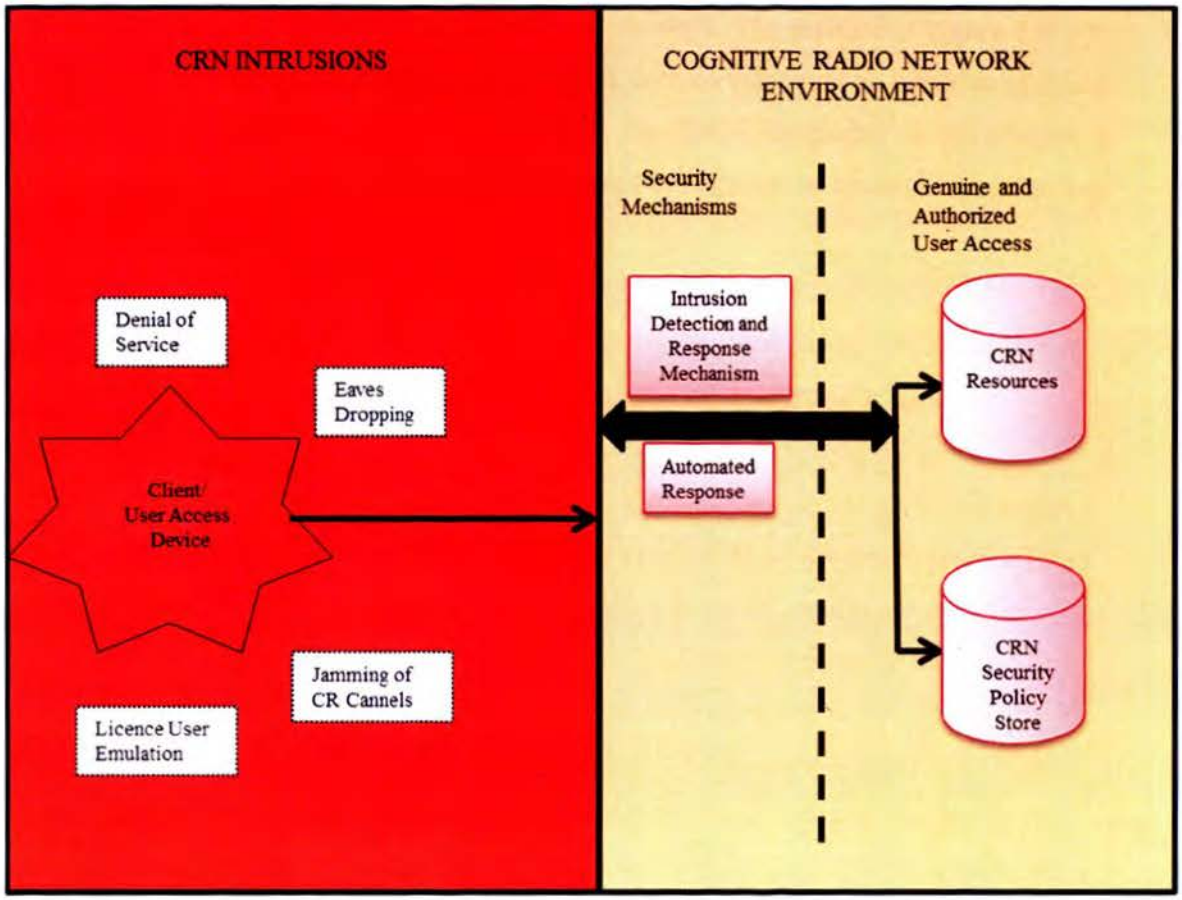


Figure 3.5 Scenario for Intrusion Detection using IDRM

Any of the various intrusions can be launched via the user access which can be any form of wireless or mobile device. Intrusions have been a constant danger to CRNs and have received increased attention as they can lead to a severe loss of revenue if a site is taken offline for a substantial period of time. The economic dividends provided by the innovation of CRN are not achieved. The target of the intrusion is to establish unauthorized access to the networks services and resources. The IDRM at interception performs proper analysis on the captured data packets, identifies the intrusions and sends quick automated responses to the intruder's device. This means that the IDRM does not allow the intruder to have access to the resources made available by the CRN. Detection of intrusion is done by enforcing the networks specification (service and security policy) on all system calls. Only the genuine and authorized users or clients are allowed access to

the CRN resources. However, no specific intrusion or attack is implemented in chapter four as this is not within the scope of this research work. The essence of Figure 3.4 is to show the IDRM reactions within the CR network domain whenever an intrusion or attack is launched from any user network. Therefore, the IDRM developed in this chapter is implemented in chapter four as a proof of concept in response to research objective four (4).

3.9.1 IDRM Scenario

Scenario Name:	NWU Student accessing the EmGEE-CR network.
Participating Actor:	Baxilo.
Flow of Events:	Baxilo, an EmGEE-CRN client, request for access to the network server and appends an attack [sends packets (data and information) which does not conform to what the company approves]. The IDRM detects the intrusion and quickly disallows access by sending access disallowed response and warning to the user's device to stop the attack. Vital information about the attack is stored in the intrusion detection database for further investigations by the network security administrator. But, if the information corresponds with the security data or service profile in the database, access allowed response is sent by the IDRM.

3.10 Rationale of IDR Model

The purpose of the model in the context of this research project is to ensure a secure communication using intrusion detection and response model as the best security approach for cognitive radio networks. It monitors network traffic and analyses packet data along the lines of transmission at all layers of the network so as to detect intrusions and stop them from escalating and disrupting the flow of communication within the

networks. However, the model can operate as network based to provide an effective detection capability and dual benefits. However, operating as a hybrid system:

(a) The model can reside on any computer or devices connected to segment of the CR network to look for signs of attacks while examining packets for attack patterns and watching traffic going into and out of the network segment.

(b) The model can provide special implementation of TCP/IP stack by using protocol stack verification to locate invalid data packets and unexpected packet behaviour or improper use.

(c) The model can be installed on a particular computer or server and monitors activity only on that system monitor the status of key system files in order to detect when intruder creates, modifies, or deletes any file.

(d) The model is capable of accessing encrypted data and information travelling over the network. It can also operate on the principle of configuration or change management.

3.11 Chapter Summary

Presented in this chapter is the state-of the-art on security in CRNs followed by the vulnerabilities and attacks in CRNs. The various CRNs security requirements for developing IDRM and the IDRM design were also reported.

CHAPTER FOUR

IMPLEMENTATION AND RESULT ANALYSIS

4.1 Chapter Overview

This chapter presents the implementation and result analysis of the intrusion detection and response model (IDRM) as a security mechanism to enhance security in cognitive radio networks. This is achieved by transforming the information from the requirement analysis and the developed IDRM model reported in chapter three. The IDRM is a security infrastructure that is capable of monitoring the entire network to detect unwanted, unauthorized malicious use of the CR network. It generates and sends a quick automated response and gives a warning once an intrusion, malicious act or an unauthorized activity is detected within and outside the CR network. This automated response restricts the intrusion from escalating in the network without human intervention. Reported in this chapter are the interface relationships that describe the operation and different functionalities of the IDRM as specified in the requirements and use case presented in 3.5 and 3.6 respectively.

4.2 Model Implementation Phase

In this implementation phase, no specific intrusion or attack is implemented as this is not within the scope of this research work. Rather, the IDRM is implemented in response to research objective 4. The IDRM is configured to monitor the activity of the EmGEE-CRN. It acts as a packet analyser that analyses the nodes' communication with each other, coordinator or router in real time. The packets (data and information) captured are compared to the knowledge base of intrusion specification and the service and security policy that were previously programmed by the network. Mainly, the IDRM is set to detect any packet whose format did not comply with what is approved by the network and to generate automated responses as specified in Table 3.7 and Figure 3.2. The implementation phase shows the several automated responses generated and sent by the IDRM to stop the intrusion and ward off the intruders. The aim is to proof the concept of intrusion detection and response model (IDRM) for cognitive radio networks as specified

in objective 4. This indicates that the services provided by the network are monitored and controlled using IDRM access control mechanism as a detective measure against intrusions and malicious users.

The implementation is done using Baxilo as the intruder, as indicated in Figure 4.3. He appends an intrusion to the EmGEE-CR network. The IDRM monitoring the network ensured that all system calls conforms to the predefined and specified information in the control store (intrusion specification database and the service and security policy). This enforcement policy enables the IDRM to detect the intrusion and send automated response messages as shown in the corresponding interfaces in section 4.3.

4.3 Result Analysis Phase

The result analysis is presented using various interfaces shown below. The interfaces include: the EmGEE-CRN home page, the EmGEE-CRN login page, access disallowed, access allowed, the EmGEE-CRN welcome page, the EmGEE-CRN site administrator's and the intrusion detection database respectively. However, these automated responses are generated and sent by the IDRM to the appropriate destinations without any human intervention.

4.3.1 EmGEE CRN Home page

The home page of EmGEE CRN Company is the main page of the network, which is the entry point to the Cognitive radio infrastructure.

Figure 4.1: EmGEE-CRN Home page

It consists of the login button, the register button, including sites of interest shown in Figure 4.1 and other vital information about the services rendered by the company.

4.3.2 Login Page

When a request for services is initiated, the client would need to login to the system by supplying identification details (username and password) as shown in Figure 4.2.

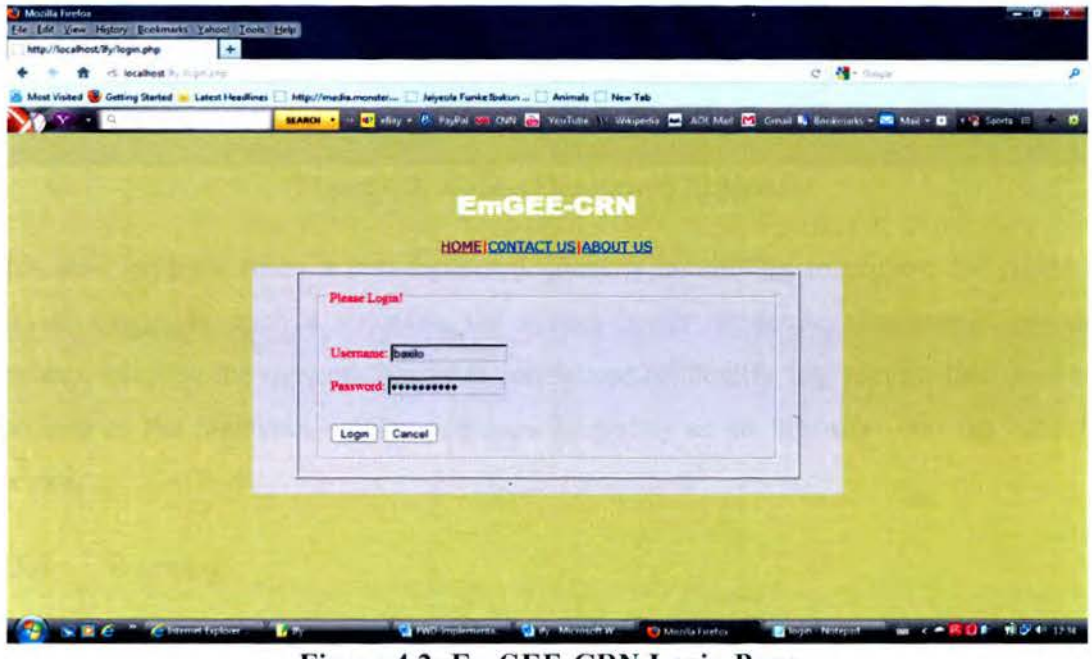


Figure 4.2: EmGEE-CRN Login Page

The details would then be verified and validated from information already stored in the CRN client registration or membership database.

4.3.3 Access Disallowed

The intruder (Baxilo) requests for access to the EmGEE-CRN as indicated in the IDRM UML diagram in Figure 3.4 and the intrusion scenario in section 3.10.1. The IDRM analyses the details supplied and the form of entry based on the service and networks security policy and identifies an intrusion. Consequently, an automated access disallowed response is generated by the IDRM and sent to the Baxilos' device as displayed in Figure 4.3. This automated access disallowed response signifies that IDRM has disconnected the intruder (Baxilo) from the network.

Figure 4.3: Access Disallowed Response

This also happens when a non-registered client is attempting to request for rights of service usage. In such a situation, the system sends an access disallowed response message because the network has been configured to identify any request that does not conform to the networks service and security policy as an intrusion into the network service.

4.3.4 Warning

The IDRM also sends a warning message to the intruder's device as shown in Figure 4.3.

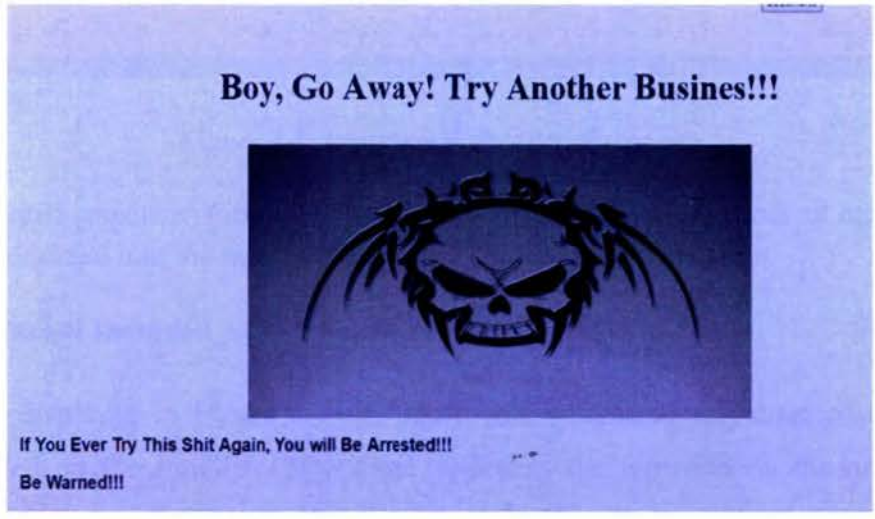


Figure 4.4: Warning Response

This warning response provided by the IDRM is easy to understand and it shows that the IDRM has disallowed the intruders' access to the network, the packet has been dropped and the port is also shut down. It scares the intruders away from the network for fear of their identity being disclosed.

4.3.5 Intruders Forbidden

The page displayed in Figure 4.5 is one of the automated responses of the IDRM. When an access disallowed message and a warning message is sent to the intruder's device, the response as shown in the Figure 4.5 is also sent to the intruder. It automatically keeps the intruder off the network access.

Figure 4.5: Intruders Forbidden Response

The automated response "forbidden" implies that the IDRM ensures that all unauthorized access is restricted into the network to enhance secured communication.

4.3.6 Packet Dropped

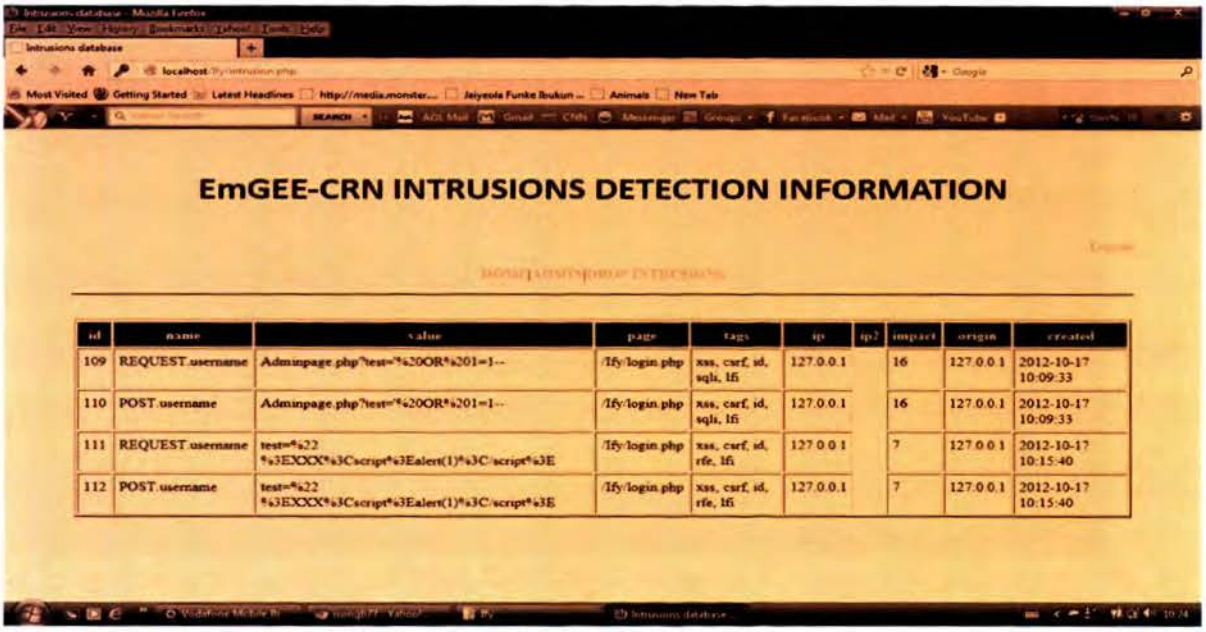
This page displayed in Figure 4. 6, is one of the automated responses of the IDRM implemented on the EmGEE-CRN. Once it detects the intrusion on the network, an access disallowed message is displayed on the intruder's device which indicates that the IDRM is active on its monitoring and analysis responsibility.

Figure 4.6: Packet Dropped

The next automated action after sending a disallowed message is to drop the packets and shut down the port and send the information to the network security administrator. Apparently this keeps the networks security administrators (NSAs) informed of the intrusion incidences or activities in the network and helps them for further investigations. The "packet dropped" interfaces is as shown in Figure 4.6.

4.3.7 Intrusions Database Log

The Intrusion Database Log as displayed Figure 4.7 is a collection of predefined intrusion patterns or specifications that have already been defined, classified and also information about detected intrusion detected in the EmGEE-CRN. It indicates malicious activities, attacks and intrusions in the EmGEE-CRN. Once the analysis engine examines traffic, it matches the pattern with the appropriate attack or intrusion specifications and information recorded in the database. It can contain as many attributes as possible depending on the storage capacity provided.



id	name	value	page	tags	ip	ip2	impact	origin	created
109	REQUEST.username	Adminpage.php?test='%20OR'%201=1--	/Ify/login.php	xss, csrf, id, sqli, lfi	127.0.0.1		16	127.0.0.1	2012-10-17 10:09:33
110	POST.username	Adminpage.php?test='%20OR'%201=1--	/Ify/login.php	xss, csrf, id, sqli, lfi	127.0.0.1		16	127.0.0.1	2012-10-17 10:09:33
111	REQUEST.username	test=%22 %3EXXX%3Cscript%3Ealert(1)%3C/script%3E	/Ify/login.php	xss, csrf, id, rfe, lfi	127.0.0.1		7	127.0.0.1	2012-10-17 10:15:40
112	POST.username	test=%22 %3EXXX%3Cscript%3Ealert(1)%3C/script%3E	/Ify/login.php	xss, csrf, id, rfe, lfi	127.0.0.1		7	127.0.0.1	2012-10-17 10:15:40

Figure 4.7: Intrusions Database Log

The entry table in Intrusions Database Log is specified using: id; name; value; page; tag; ip; ip2; impact; origin and created. The 'id' details are used to identify a particular intrusion in the intrusions database, the name is used to identify the intruder's device, the value is used to identify EmGEE-CRN host device that is the target point of the intrusion, the 'page' identifies the entry point of the intruder, the 'tags' is used to identify the attributes of the attacks, the 'ip and ip2' is used to identify the particular IP address in the EmGEE-CRN through which the packets were transmitted, the 'impacts' is used to identify the 'impact' of IDRM in detecting the intrusion, the 'origin' identifies where the intrusion originated from and, 'created' holds the time at which the intrusion was captured and recorded in the database.

4.3.8 Access Allowed

The client is allowed to successfully login if he can be identified from the database information as a genuine user of the EmGEE-CRN as shown in Figure 4.8, otherwise access is disallowed. In a situation where the clients login details can be verified and validated, an automated response in form of an allowed messaged is displayed and the user can have access to the EmGEE-CRN resources for which he or she is authorized to access.

Figure 4.8: Access Allowed

But, if the details supplied cannot be verified the IDRM monitoring and analysing data and information transmitted across the network identifies it as an intrusion. This implies that the request is invalid; therefore IDRM blocks the port (access). Then, an automated response in form of a disallowed access message is displayed and a warning is sent alongside to the intruder.

4.3.9 Welcome page

This page is displayed when a registered member clicks the 'About us' and 'Contact us' button from the home page in Figure 4.1.

Figure 4.9: Welcome Page

All the necessary information about the operations, services, and resources provided by EmGEE-CRN is displayed as shown in Figure 4.9. The contact information can also be viewed from this domain. From this window clients can navigate to any part of the network domain, provided they have the access privilege to the resources made available in such network domain.

4.3.10 EmGEE-CRN Services

The page in Figure 4.10 displays both the services offered by the EmGEE-CRN and the available services at the time the service button is clicked. Via this interface, access to the networks resources can be obtained for an allowed user.

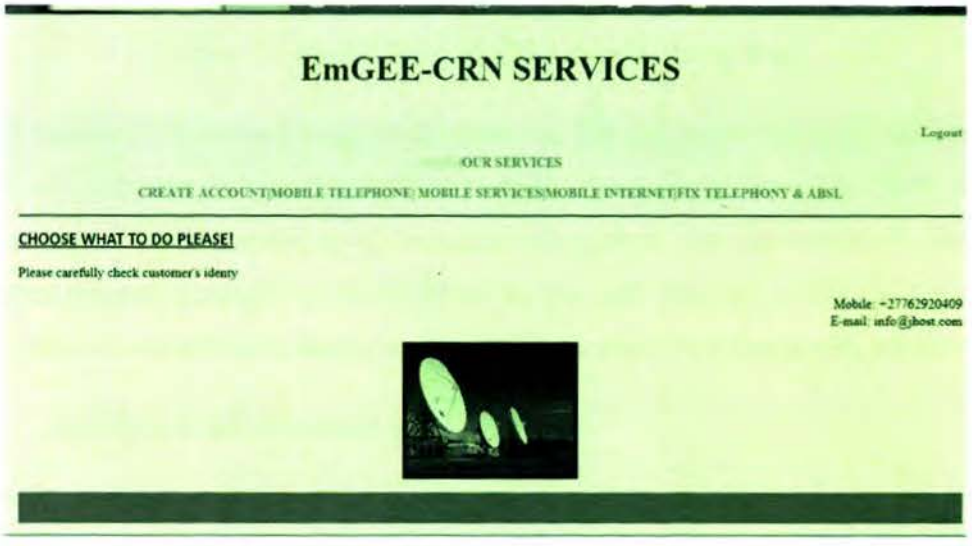


Figure 4.10: EmGEE-CRN Services

This implies that an authenticated or genuine user must be authorized to access any of the services provided by the network before access to that network domain is granted. Services or resources to access are specified at the registration window and stored in the database for the purpose of verification.

4.3.11 EMGEE-CRN Site Administrator Page

The page in Figure 4.11 shows that the EmGEE-CRN security administrator has access right to networks database and the clients' identity (password) database.

Figure 4.11: EMGEE-CRN Site Administrator Page

When it is viewed from the intrusions database log that the registered or authorized users devices or networks are being used to launch attacks, the EmGEE-CRN security administrator has the capability to automatically delete the account and disable or disconnect the root connections to the client or the user from accessing the network to ensure efficient and effective access control to enhance security and quality of service.

4.3.12 EmGEE-CRN Database

The basic information required for the registration of the clients based on the network service and security policy is captured from this window and stored in the database as shown in Figure 4.12. This information is required for verification to enable intrusion the IDRM detect intrusion in real time. Figure 4.12 represents the authorized users' management database. It consists of profiles of all the registered clients of the network, which includes: the clients name, service name, service ID, password, e-mail and year of registration. These are clearly specified and stored in this domain for authentication, authorization and security policy services.

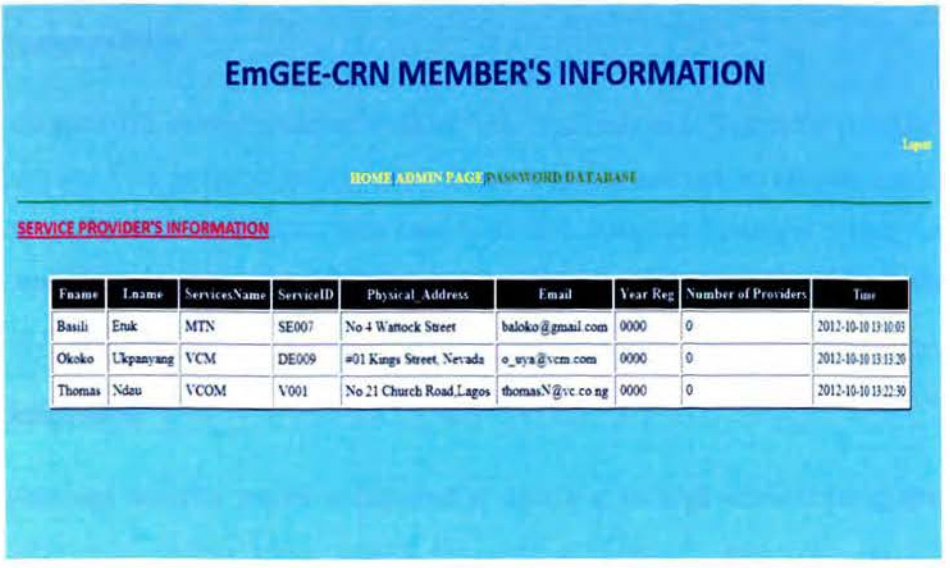


Figure 4.12: EmGEE-CRN Database

When a request for services is initiated, the client would need to login to the system by supplying identification details (username and password). The details would then be verified and validated from information already stored in the CRN client membership information database. An access allowed response is sent only if the user is who he claims to be as verified and validated from the database information. In situation where access is disallowed, it implies that the request is invalid and the user is identified as an intruder.

4.4 Model Evaluation

Having implemented the IDRM system and analysed the results obtained, it is imperative to evaluate the model based on the fundamental network security objectives for CRNs and the model capability measures.

4.4.1 Model Capability Measures

In this section the underlying capabilities of a secured communication network are specified to enable the designing of a security model for data and information management in CRNs. The capabilities include interoperability, integration, trust relationship, flexibility and efficiency. These capabilities ensure reliability, availability and quality of the network service.

(i) Interoperability

Secured network communication enables host systems and devices in the network to interoperate. This is the capability that allows multiple entities in different domain and hosting environment to interact with each other and exchange messages to identify a user from one domain in another domain, having a central database. It enhances efficient sharing of resources within the network environment.

(ii) Integration

The proposed security model is required to enable a secured communication network, integration and compatibility among the host environment and other new security mechanisms that will be incorporated as the network expands.

(iii) Trust Relationship

A trust relationship exists in an atmosphere of a secured communication network. It is necessary to establish a trust agreement and relationship between different entities and several components in a distributed network for sharing data and information. It also assists in determining identity profile and security data when necessary. It guarantees and promotes confidence for effective interactions. CRN is a dynamic and multiuser system. Consequently, this capability enables efficient and effective resource control stages or processes as used in this research project, such as connection request for authentication and resource request for authorization, and decision stage by the server host based on the particular resource the client requests for. However, all the components of authentication and authorizations are carefully specified in order to develop a reliable framework.

(iv) Flexibility

The model is able to cope with different network topologies and is also able to express the dependencies among resources themselves and between services and users. It reflects the actual security needs of the network and it's able to determine the appropriate response actions accurately.

(v) Efficiency

The model monitors and analysis data packets quickly and responds very fast in order to keep the time window of vulnerability and intrusion small. All automated responses are generated and sent as quick as possible.

4.4.2 IDRM Deployment

Decision about where to locate elements of the intrusion detection and response model in a CRN is very important for effective and efficient impact. Planners must select a deployment strategy that is based on careful analysis of the company's network and information security requirements that enhances its overall security. However four locations are recommended for IDRM sensors in CRN.

Location 1: Behind each external firewall.

Location 2: Outside an external firewall.

Location 3: On major network backbones.

Location 4: On critical subnets.

Deployment begins with implementing most critical systems first. Installation continues until either all systems are installed or the organization reaches planned degree of coverage it wants to operate with.

4.4.3 Benefits of IDRM

The capabilities of IDRM enable it to perform the following functions well:

(i) Monitors and analyses network events and user behaviours.
(ii) Tests security states of network configurations.
(iii) Baselines security state of network and tracking changes.
(iv) Recognizes system event patterns matching known attacks.
(v) Recognizes activity patterns that vary from normal activity.
(vi) Manages OS audit and logging mechanisms and data they generate.

(vii) Takes appropriate automated responses to stop the intrusions or attacks that are detected.

(viii) Sends intrusion information to the administrators when intrusions are detected.

(x) Measures enforcement of security policies encoded in analysis engine.

(xi) Provides default information security policies.

(xii) Allows network security administrators to perform further security investigations.

4.5 Chapter Summary

In this chapter, an intrusion detection and response model that forms the security infrastructure to enhance security in CRN was presented. It demonstrates how the model is implemented by transforming the artefacts from the requirements analysis reported in chapter three. The IDRM operates using EmGEE-CRN as a network domain for implementation. Consequently, this research project presents IDRM as a reliable security infrastructure to enhance security in cognitive radio networks by preventing intrusions, unauthorized access and all forms of malicious use of the spectrum resources in other to ensure quality of service (QoS).

CHAPTER FIVE
SUMMARY, CONCLUSION AND FUTURE WORK

5.1 Summary

Cognitive radio offers a promise of intelligent radios that can learn from and adapt to their environment. Much research is currently underway developing various reasoning that allow cognitive radios to operate optimally. However, as with many new technologies, initial research has not focused on security aspects of cognitive radio networks. Typically, security is always "bolted on" after the fact by adding some sort of link authentication and encryption. This typically works well for data traversing a wireless network, but not necessarily for things fundamental to the operation of the wireless link itself. Since cognitive radios can adapt to their environment and change how they communicate, it is crucial that they select optimal and secure means of communications.

Moreover, with the developments of network applications, network attacks are greatly increasing both in number and severity. As a key technique in network security domain, Therefore, reported in this research project is an Intrusion Detection and Response Model 9IDRM) to enhance security in cognitive radio networks. It plays the vital role of detecting various kinds of attacks and secures the networks. Intrusion detection is defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. IDRM is typically one part of an overall protection system that is installed around a system or device. It is used to monitor networks for attacks or intrusions and generate automated responses against the intrusions whenever detected. It also reports these intrusions to the network security administrator in order to take further actions. It is not a stand-alone protection measure. The main purpose of IDRM is to find out intrusions among normal audit data and this can be considered as classification problem. As part of intrusion detection systems, it is an effective security technology, which can detect, prevent, and react to attacks. It performs monitoring of target sources of activities, such as audit and network traffic data in CRNs, requiring security measures, and employs proper techniques for providing security services.

Apparently, with this tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever. Intrusion detection is needed in today's computing environment because it is impossible to keep pace with current and potential intruders and vulnerabilities in our computing systems. The CRN domain is constantly evolving and changing field by new technology and the internet. Hence new attacks replicate on daily basis. Therefore intrusion detection systems are used in managing threats and vulnerabilities in the changing environment.

Attacks on computer network systems can be devastating and affect networks and corporate establishments. We need to curb these attacks by installing IDRM to identify the intrusions. Without the use of IDRM to monitor network activities, intrusions which can possibly result in irreparable damage to an organization's network can occur.

5.2 Conclusion

Since Intrusion Detection (ID) is such an important technology, this research successfully created a network-based Intrusion Detection and Response Model. Automated response to intrusions is becoming a critical issue to defending network systems and operations. Since the attacker can take actions at computer speeds, intrusion detection systems (IDS) need the capability to react without human intervention. This is why a model that supports development of automated response cannot be avoided. This model allows easy integration of detection and response components to enable testing with automated response strategies. Again, because intrusion detection systems (IDSs) have reached a high level of sophistication and are to detect intrusions with a variety of methods, systems administrators neither can keep up with the pace at which the IDS is detecting intrusions nor delivering response (alerts). In case of an identified intrusion, these response components have to initiate appropriate actions to counter emerging threats and reported in this research is the development of an Intrusion Detection System and its response Model called IDRM to enhance Security in Cognitive Radio Networks.

5.3 Future Work

While this IDRM is useful, it will extend its application in the near future to following arrears of interest:

(i) Identify realistic operational scenarios to identify which security threats will be more relevant for the end-users.

(ii) Investigate the performance impact of protection security solutions in SDR platform to guarantee that real-time requirements are still validated.

(iv) Design tamper-resistance modules to enforce the spectrum regulation policies in the SDR device.

(v) Investigate the performance and efficiency of protection techniques based on collaborative spectrum sensing for a realistic deployment.

(vii) Further research on protection techniques against threats to the cognitive engine is needed.

REFERENCES

[1] J. Mitola, and G. Q. Maguire. "Cognitive radio: Making Software Radios more Personal." *IEEE Journal on Network Communication*, vol. 6, pp. 13–18, Aug. 1999.

[2] B. Wang, and K.J.R. Liu."Advances in Cognitive Radio Networks: A Survey." *IEEE Journal on Advancement in Cognitive Radio*, vol. 5, pp. 5-3, Feb, 2011.

[3] S. Haykin, "Cognitive radio: brain-empowered wireless communications." *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 201–220, Feb. 2005.

[4] G. Baldini, S Braghin, A. Trombetta, and Nai Fovino . "Adaptive and Distributed Access Control in Cognitive Radio Networks," in *Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications,* 2010, pp. 115-122.

[5] J. Hwang, and Y. Hyenyoung. "Dynamic Spectrum Management Policy for Cognitive Radio: An Analysis of Implementation Feasibility Issues" *in Proceedings of IEEE DySPAN Symposium*, 2008, pp.115-126.

[6] P. Steenkiste, D. Sicker, G. Minder, and R. Dipankar. "Future Directions in Cognitive Radio Network Research," in *Proceedings of NSF Workshop Report*, March 9-10, 2009, pp. 1-3.

[7] T. X. Brown, and A. Sethi. "Potential Cognitive Radio Denial of-Service Vulnerabilities and Protection Countermeasures: A Multidimensional Analysis and Assessment," *in Proceedings of the International Conference of Cognitive Radio Oriented Wireless Networks and Communications,* 2007, pp. 456-464

[8] A. A. Ghorbani. "Network Intrusion Detection and Prevention: Concepts and Techniques." *The International Journal of Information Security,* vol. 47, pp. 27-48, May, 2010.

[9] T. Charles Clancy, and N. Goergen, "Security in Cognitive Radio Networks: Threat and Mitigation," in *Proceedings of the 3rd International Conference on Cognitive Oriented Wireless Networks and Communications,* 2008, pp. 215-220.

[10] R. Chen, P. Jung-Min, and H. Jeffrey Reed, "Defence against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE journal on selected areas in Communications, vol. 26,*pp. 315-323, January 2008.

[11] T. Xiaoyong, L. Kenli, Z. Zeng, and B. Veeravalli. "A Novel Security Driven Scheduling Algorithm for Procedure Constrained Tasks in Heterogeneous Distributed Systems." *IEEE Journal*, vol. 60, pp. 1017-1029, July, 2011.

[12] H. Fuping, S. Wang, and Z. Cheng. "Secure Cooperative Spectrum Sensing for Cognitive Radio Networks," in *Proceedings of IEEE Military Communication Conference*, 2009, pp. 1-7.

[13] P. Ank. "Cognitive Radio Defying Spectrum Management," in *Proceedings of CRNI Conference*, 2008, pp.2-6.

[14] B.O Pages, I. Foster, F. Siebenlist, and A. Rachans. " A Multipolicy Authorization Framework for Grid Security," in *Proceedings of the Fifth IEEE Symposium on Network Computing and Application*, 2006, pp.269-272.

[15] T. Newman, C. Clancy, M. McHenry, and J. Reed."Case Study: Security Analysis of a Dynamic Spectrum Access Radio System," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM)*, 2010, pp. 1120-1125.

[16] D. Denning, and E. Dorothy. "An Intrusion Detection Model,"in *Proceedings of the Seventh IEEE Symposium on Security and Privacy*, 1986, pp. 119–131.

[17] D. Anderson, T. Frivold, A. Tamaru, and A. Valdes. " Next Generation Intrusion Detection Expert System (NIDES), "in *Proceedings of the SRI International Conference,* 1994, pp. 445-456.

[18] Y. Zhang, W. Lee, and Y. Huang. "Intrusion Detection Techniques for Mobile Wireless Networks." *Wireless Networks Journal,* vol. 9, pp. 545-556, 1999.

[19] P. Albers, and O. Camp. "Security in Ad-hoc Networks: A general Intrusion Detection Architecture Enhancing Trust Based Approaches," in *Proceedings of the first International Workshop on Wireless Information Systems,* 2002, pp. 1-12.

[20] Y. Zhang, and W. Lee. "Intrusion Detection in Wireless Ad-hoc Networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking,* 2000, pp. 275- 283.

[21] V. Sharma, and Y. S Mann. "*Emerging Technologies in Web Intelligence*." *Infosys Technologies Journal*, vol.2, pp. 115-121, May 5, 2010.

[22] B.O Pages, I. Foster, F. Siebenlist, and A. Rachans. "A Multipolicy Authorization Framework for Grid Security," in *Proceedings of the Fifth IEEE Symposium on Network Computing and Application*, 2006, pp.269-272.

[23] M. McHenry, Z. Youping, and O. Haddadin, "Dynamic Spectrum Access Radio Performance for UAS ISR Missions," in *Proceedings of the Military Communication Conference,* 2010. pp. 2345-2350.

[24] J. Wang. *Computer Network Security*. Beijing: Higher Education Press and New York: Springer Berlin Heidelberg, 2009, pp. 3-24.

[26] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle. "GrIDS - A Graph-Based Intrusion Detection System for Large Networks", in *Proceedings of the 19th National Conference on Information Systems Security*," 1996, pp. 120-127.

[27] R. Roman, J. Zhou, and J. Lopez. "Applying Intrusion Detection Systems to Wireless Sensor Networks," in *Proceedings of 3rd IEEE Consumer Communications and Networking Conference,* 2006, pp. 550-557.

[28] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey." *International Journal on Computer networks*, pp. 2127-2159, 2006.

[29] M. Sherman, A. Mody, R. Martinez, and C. Rodriguez, "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence,"*IEEE Communication Magazine*, 2008, pp. 626-634.

[30] G. Radhaman, G.S.V. Radha, and K. Rao. *Web Service Security and E-business*. 701 E. Chocolate Avenue, Hershey, USA: Idea group publishing, 2oo7, pp. 129-131.

[31] T. Abbes, A. Bouhoula, and M. Rusinowitch. " Protocol Analysis in Intrusion Detection Using Decision Tree," in *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC)*, 2004, pp. 207-215.

[32] C. Endorf, E. Schultz, and J. Mellander. *Intrusion Detection and Prevention*. Fort Washinton, PA: McGraw-Hill, 2004, pp. 193-219.

[33] L. Herberlein, and G. Dias. "A Network Security Monitor," in *proceedings of the IEEE Symposium on Security and Privacy*, 1990, pp. 296-304.

[34] D. Sterne, and P. Balasubramanyam. " A General Cooperative Intrusion Detection Architecture for MANETs," in *Proceedings of the 3rd IEEE International Workshop on Imation Assurance*, 2005, pp. 57-70.

[35] B. Sun, K. Wu, and U. W. Pooch. "Alert *Aggregation* in Mobile Adhoc Networks," in *proceedings of the 2003 ACM Workshop on Wireless Security in Conjunction with the 9th Annual International Conference on Mobile Computing and Networking*, 2003, pp. 67-78.

[36] A. Fragkiadakis, V. Siris, and N. Petroulakis. "Anomaly Based Intrusion Detection Algorithms for Wireless Networkks," in *Proceedings of the 2009 World Computing Conference*, 2009, pp. 115-122.

[37] A. Fragkiadakis, E. Tragos, T. Tryfonas, and I. Askoxylakis. " Design and Performance Evaluation of a Light Weight Wireless Early Warning Intrusion Detection Prototype." *EURASIP Journal on Wireless Communication and Networking*, vol. 25, pp. 50-55, 2011.

[38] M. Thermilarus, S. Mishra, and R. Sirdhar. "A Cross Layer Approach to Detect Jamming Attacks in Wireless Ad hoc Networks," in *Proceedings of MILCOM Conference*, 2006, pp. 1-7.

[39] S. Frankel, B. Eydt, L. Owens, K. Scarfone. "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," *NIST Special Publication*, 2007, pp. 119-105.

[40] S. Kumar. "*Classification and Detection of Computer Intrusions," Ph.D. Thesis*, Department of Computer Sciences, Purdue University, W. Lafayette, 1995.

[41] T. Bass. "Multi-sensor Data Fusion for Next Generation Distributed Intrusion Detection Systems," in *Proceedings of IRIS National Symposium on Sensor and Data Fusion*, 1999, pp. 550-557.

[42] G. Helmer, Johnny S.K. Wong, V. Honavar, and L. Miller. "Lightweight Agents for Intrusion Detection." *Journal of Systems and Software,* vol. 2, pp. 660-666, 2000.

[43] J. Mintola." Licentiate Thesis: *Cognitive Radio, Model Based Competence for Software Radio.*" Depatment of Tele Informatics, Computer Communications Systems, Stockholm, Sweden, 1999.

[44] S. Kumar Sarkar, T.G. Basavaraju, and C. Puttamadappa. *Ad Hoc Mobile Wireless Networks*. Hershey Avenue, New York: McGraw Hill Publishing Company, 2006, pp.229-231.

[45] J. Slay, and A. Koronios. *Information Technology, Security and Risk Management*. 44 Casmire. Australia: John Willy and Sons Company, 2006, pp. 560-580.

[46] A. Sethi, and T.X. Brown. "Hammer Model Threat Assessment of Cognitive Radio Denial of Service Attacks," in *Proceedings of the 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Oct. 2008, pp.1-12.

[47] Y. Zhang, X. Gaochao, and G. Xiaozhong. "Security Threats in Cognitive Radio Networks," in *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications*, Sept. 2008, pp. 1036-1041.

[48] S. Arkoulis, L. Kazatzopoulos, C. Delakouridis, and G.F. Marias. "Cognitive Spectrum and Its Security Issues," in *Proceedings of the 2nd International Conference on Next Generation Mobile Applications, Services and Technologies*, Sept. 2008, pp.565-570.

[49] J. L. Burbank. "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," in *Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, May 2008, pp. 1-7.

[50] Z. Jin and K. Subbalakshmi. "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," in *Proceedings of ICC*, 2009, pp. 1–5.

[51] Z. Jin, S. Anand, and K. Subbalakshmi. "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," in *Proceedings of ACM SigMobile Computing and Communication Review*, 2009, pp. 74–85.

[52] Y. Liu, P. Ning, and H. Dai. "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in *Proceedings of 2010 IEEE Symposium on Security and Privacy*, 2010, pp. 286–301.

[53] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez. "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proceedings of IPCCC*, 2009, pp. 208–215.

[54] C. Mathur and P. Subbalakshmi. "Digital signatures for centralized DSA networks," in *Proceedings of 1st IEEE Workshop on Cognitive Radio Networks,* 2007, pp. 1037–1041.

[55] W. Wang, H. Li, Y. Sun, and Z. Han. "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proceedings of CISS*, 2009, pp. 130–134.

[56] H. Li and Z. Han. "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in proceedings of DySPAN, 2010, pp. 1–12.

[57] F. Zhu and S. Seo. "Enhanced robust cooperative spectrum sensing in cognitive radio." *Journal of Communications and Networks*, vol. 11, pp. 122–133, 2009.

Appendix: Source Code

```
!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<head>

<style type="Text/CSS">
body
    {
color: black;
background: BurlyWood ;
font-family: verdana, geneva, arial, helvetica, sans-serif, Candara;
font-size: 10 pt;
        text-align: justify;
margin-left: 72px;
        margin-right: 72px;
        padding: 0;

        }

   h1
{ color:GREEN;
        text-align:center;
        font-family: Verdana;
        font-weight: bold;
        font-size: 28px;
        text-transform: uppercase;
        }
  h2
{ color:Red;
        text-align:center;
        font-family: Arial;
        font-weight: bold;
        font-size: 15px;
        text-transform: uppercase;
        }
  h3
{ color:GOLD;
        text-align:center;
        font-family: Arial;
        font-weight: bold;
        font-size: 10px;

        }
 h4
{ color:MAROON;
```

```
        text-align:center;
        font-family: Arial;
        font-weight: bold;
        font-size: 18px;
        text-transform: uppercase;
        }
#header{
        width: 100;
        height: 0px;
        min-width: 565px;

} /* end header styles */
p {
font-size: 15px;;
font-family: Verdana, Tahoma, Arial, sans-serif;
}

p.copyright

        {
        font-family: Arial;
        font-size: 12px;
        color: white;
        background: teal;}
        }

.navbar {
        background-color: #CCC;
        border-bottom: #999;
        border-left: #999;
        border-width: 0 0 thin;
        border-style: none none groove;
        display: block;
        float: left;
        margin: 0 0 0 10px;
        padding: 0 10px 0 10px;
        width: 100px;
        }

#item {
        text-align: justify;
        width: 100%;
        height: 160px;
}

#leftColumn {
        float: left;
        width:190px;
        text-align: left;
}
```

```
#rightColumn {
        text-align: left;
        float: left;
        margin-left: 50px;
        width: 500px;  }

a        {text-decoration: none; font-weight: bold; background: transparent;}
a:link
        {color: olive;}
a:visited
        {color: WHITE;}
a:hover {color:Magenta ; text-decoration: underline}

</style>

<title>EmGEE HOMEPAGE</title>

</head>

<body>

<h1>EmGEE - CRN </h1>

<div id="header"><imgsrc="images/tele.jpg" align= "le" width="150" height="90"border="0"
alt="logo" /></div>

<table border="0" cellpadding="0" cellspacing="0"width="1000" align="center">

<tr height="90">

<td width="100" height="100" ALIGN=CENTER VALIGN=TOP bgcolor="Lavender " font
color="white">

<div class="navbar">

<p align="center"><a href="#Hompe page">HOME</a></p>

<p align="center"><a href="contact.php"> CONTACT US</a></p>

<p align="center"><a href="about.php"> ABOUT US </a></p>

<p align="center"><a href="login.php">EmGEE-CRN SERVICES </a></p>

</div>

</td>

<td width="400" height="400" VALIGN=TOP bgcolor="Cornsilk "rowspan="3">

<div id="item">
<div id="leftColumn">
```

```
<h2>EmGEE-CRN </h2>
<imgsrc="images/guiset.jpg" alt="Animals" width="190" height="146">
</div>

<div id="rightColumn">

<p>EmGEE-CRN offers variety of services to wide range of customers ranging from supports, authentication, authorization etc.</p>

<p><a href="http://www.arclightrecords.com"> Click Here To View Website</a></p>
</div>
</div><!-- end Arclight item -->

<div id="item">
<div id="leftColumn">
<h2> WILD LIVE RESERVE </h2>
<imgsrc="images/tigers.jpg" alt="Animals" width="190" height="146">
</div>
<div id="rightColumn">

<p>We also promote tourism and hotel servise to tourists world wide. </p>

<p><a href="http://www.arclightrecords.com"> Click Here To View Website</a></p>
</div>
</div><!-- end Arclight item -->

<div id="item">
<div id="leftColumn">

<h2> CAR RENTALS </h2>
<imgsrc="images/car.jpg" alt="Animals" width="190" height="146">
</div>
<div id="rightColumn">

<p>We also provides car rental services to our customers/visitors. In stock, we have various brands and models of cars</p>

<p><a href="http://www.arclightrecords.com"> Click Here To View Website</a></p>
</div>
</div><!-- end Arclight item -->
<br>
<div id="item">
<div id="leftColumn">
<h2> SERVICE PROVIDERS </h2>

<h3> MICROSOFT </h3>

<imgsrc="images/micro.jpeg" alt="Animals" width="190" height="146">
</div>
<div id="rightColumn">
```

```
<p> Our Service provider, MICROSOFT provides lots of support services to our clients world wide.</p>

<p><a href="http://www.arclightrecords.com"> Click Here To View Website</a></p>
</div>

</div>

</td>
</tr>

<tr>
<td height="80" width="100" align= "center" VALIGN=TOP type="text/css" style="background-color: DarkSeaGreen ; color: white; font-weight: bolder;">
<h2>Member Login</h2>
<div class="navbar">

<p align="center"><a href="login.php">LOGIN</a></p>

<h2> New Member Registeration</h2>
<p align="center"><a href="register.php"> REGISTER</a></p>

</div>
</td>
</tr>

<tr>
<td height="80" width="100" align= "center" VALIGN=TOP type="text/css" style="background-color: Aquamarine ; color: white; font-weight: bolder;">
<h2> Sites of Interest </h2>

<div class="navbar">

<p align="center"><a href="http://www.google.com"target="_blank">Google</a></p>

<p align="center"><a href="http://www.amazon.com"target="_blank">Amazon</a></p>

<p align="center"><a href="http://www.yahoo.com"target="_blank">Yahoo</a></p>

<p align="center"><a href="http://www.ebay.com"target="_blank">Ebay SA</a></p>

<p align="center"><a href="http://www.nwu.ac.za/"target="_blank">North-West University</a></p>

</div>

</td>
</tr>

</table>
```

```
<p class="copyright" align="center">CopyRight (C) 2012</p>

</body>

</html>

<?php

include("config.php");

//session_start();

if($_SERVER["REQUEST_METHOD"] == "POST")

{
//username and password sent from Form

$myusername=addslashes($_POST['username']);
$mypassword=addslashes($_POST['password']);


$sql="SELECT * FROM pass WHERE username ='$myusername' AND
password='$mypassword'";

$result=mysql_query($sql);

$row=mysql_fetch_array($result);

$active=$row['active'];

$count=mysql_num_rows($result);

                // If result matched $myusername and $mypassword, table row must be 1 row

if($count==1)

{

        if ($_POST['username']=="admin")

        {
        session_register("$myusername");

        $_SESSION['login_user']=$myusername;

        header("location: adminpage.php");

        }

else {
```

```
        echo "Login Successful";
         $message ='<p>ACCESS ALLOWED!!!</p>';
         //echo "<p font-size: 8 px>ACCESS ALLOWED!!!</p>";
        session_register("$myusername");

        $_SESSION['login_user']=$myusername;

        header("location: welcome.php");
        }
}

else
        {

        $message ='<p>ACCESS DISALLOWED!!!</p>';
        //echo "<p font-size: 8 px>ACCESS DISALLOWED!!!</p>";
        //echo "<p>You must enter in a correct username and password combination!</p>";

        }
}

?>
<HTML>
<HEAD>
<style type="Text/CSS">
body {
        color: RED;
        background-color: DarkKhaki  ;
        font-family: Candara, verdanahelvetica, sans-serif, ;
        font-size: 10 pt;
        font-weight: bold;
        text-align: justify;
margin-left: 72px;
        margin-right: 72px;
        margin-top: 72px;       }

        p {color: red; font-family: verdana; font-size: 8 px;}

        H1 {color: WHITE; font-family: arial; font-size: 12 px;font-weight:900;}

        H2 {color: Red; font-family: arial; font-size: 15px;}

        H3 {color: ForestGreen; font-family: arial; font-size: 11px;}

</style>
</head>
<body>
<H1 align="center">EmGEE-CRN</H1>
```

```
<p align="center"><a href="page.php">HOME</a>|<a
href="contact.php"target="_blank">CONTACT US</a>|<a
href="about.php"target="_blank">ABOUT US</a></p>

<TABLE align="center" border="0"  cellspacing="0" CELLPADDING="4" WIDTH=700 >

<TR>

<TD BGCOLOR= silver ALIGN=LEFT VALIGN=TOP WIDTH=83%>

<form action="" method="post">

<table align="center" border="0" cellpadding="20" width="600">
<tr>
<td>
<fieldset><legend>Please Login!</legend>
<table><tr><td>
<right>
<br>

   Username: <input type="text" name="username"
style="background:#bfbfbf;color:black;border-color:#212121;" onFocus="this.style.background
= '#ffffff';" onBlur="this.style.background = '#bfbfbf';">
<br>
<br>
   Password: <input type="password" name="password"
style="background:#bfbfbf;color:#212121;border-color:#212121;"
onFocus="this.style.background = '#ffffff';" onBlur="this.style.background = '#bfbfbf';">
</right>
<br>
<br>
<p><input type="submit" name="Submit" value="Login" />
<input type="reset" value="Cancel" /></p>

<br>

<tr><td align="CENTER" >

<?php

        echo $message;
?>

</td></tr>

</td></tr>

</table>

</fieldset>
```