Security Landscape of Cognitive Radio Networks

MCS

By

Syed Shoukat Hussein

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfilment of the requirements for the degree of MS in Information Security

October 2018

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Maj Syed Shoukat Hussein** Registration No. **00000201396**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have been also incorporated in the said thesis.

Signature: _____

Name of Supervisor: **Brig Imran Rashid, PhD**

Date: _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere

DEDICATION

The thesis is devoted to

MY FAMILY, TEACHERS & FRIENDS

for their guidance, support and prayers

ACKNOWLEDGMENT

First and Foremost, I would like to bow my head in humility and grace to Allah Almighty whose benevolence and mercy has no bounds, who blessed me with the Knowledge, intellect and strength that made me accomplish this wonderful phase successfully and without whose will I could not have indulged myself in this demanding work.

This research provided a chance for me to explore new avenues and facilitated me to improve my existing knowledge pertaining to Cognitive Radio Networks (CRN). I extend my gratitude to all faculty members for their unflinching efforts and remarkable commitment to impart quality knowledge which has enabled me to accomplish this study.

My greatest of appreciation and gratitude to my thesis supervisor Brig Imran Rashid, PhD for his persistent support, inspiration, trust and confidence for making this thesis possible. It was his encouragement and guidance which facilitated to formulate this research. At the same time, I am also grateful to Assistant Professor Mian Muhammad Waseem Iqbal and Lecturer Narmeen Shafqat for their time, advice and guidance. I am also obliged to my department particularly HoD and the team in general for their administrative guidance and assistance.

I am deeply grateful to my family for the encouragement, care and constant backing. Especially, I will always be indebted to my parents for their devotion and all the things they have done for me plus to my wife and kids who bore with me throughout my MS studies.

ABSTRACT

Cognitive Radio Network(CRN) is the evolution of Radio Networks and is considered as future of Radio connectivity. CRN is characterized by its heterogeneous nature where smart radios (Cognitive Radios - CR) are interconnected to interact among themselves and with their environment. In CRN paradigm, when Cognitive Radios are provided with access to spectrum holes "White Spaces" then it becomes CRN with the aim to exploit underutilized spectral space. Various standard bodies and consortium are contributing to standardizing CRN protocols and communication technologies. Unlike traditional Radios, Radio Networks and Software Defined Radios (SDR), CRN are designed to perform prescribed functionality by employing needed resources opportunistically to keep procurement and implementation cost low.

The Cognitive Radio(CR) concept is leading the way in harnessing full potential of frequency spectrum by equipping wireless devices with auto adaptability of operating parameters based on the radio environment for efficient and opportunistic utilization of the scarce radio frequency (RF) spectrum. It is bringing about a paradigm shift in how frequency spectrum could be utilized for greater efficiency and convenience by enabling unlicensed access to licensed spectral space for solving the spectrum scarcity. Where Cognitive Radios have enormous potential, they also pose many a security challenge because of devices in the network which are invasive in nature. This thesis concentrates on attacks and provides a comprehensive review of those attacks on CR and within CRN with consolidation of the methods to execute those attacks and the solutions to mitigate those attacks.

Contents

List of Figures

List of Tables

ACRONYMS

AV	Anti-Virus
BS	Base Station
CAA	Channel Assignment Attack
C-CC-S	Common-Control Channel-Saturation
CR	Cognitive Radio
CRN	Cognitive Radio Network
DS	Direct Sequence
DSA	Dynamic Spectrum Access
FCC	Federal Communications Commission (FCC)
FC	Fusion Centre
FH	Frequency Hopping
GKM	Group Key Management
IETF	Internet Engineering Task Force
ITU-R	International Telecommunications Union-Radio Sector
JFA	Jelly Fish Attack

KDA	Key Delpetion Attack
MU	Malicous User
MW	Malware
NW	Network
OFA	Objective Function Attack
OSU	Overlapping Secondary User
PDR	Packet Delivery Ratio
PRNG	Pseudo Random Number Generator
PU	Primary User
PUEA	Primary User Emulation Attack
QoS	Quality of Service
RIJ	Routing Information Jamming
RSS-I	Received Signal Strength - Indicator
SBW	Small Backoff Window
SDR	Software Defined Radio
SS	Signal Strength
SSDF	Spectrum Sensing Data Falsification
SU	Secondary User
SW	Software

Chapter 1

INTRODUCTION

1.1 The Rise - Overview

Past couple of decades has seen many new inventions, innovations and discoveries. One can easily nominate wireless technology amongst the ones which lead all the way. Employment of wireless technology has resulted in a communication revolution with use of wired telephony services almost depleting to a restricted few and an exponential growth of cellular phone services. Cellular communication is not the only advantage that this technology has brought instead sophisticated applications like Internet, adhoc networks, Internet of Things (IoT), cloud computing etc. partly or solely involve the use of this technology.

The sudden boom of applications involving the employment of wireless technology naturally led to the exhaustion of spectral space and resultantly leading the researchers to focus on acute shortage of wireless spectrum. The increasing demand of usable spectrum range has rung many an alarm bells in the world of spectral space due to serious spectrum shortage which is getting acute day by day. Low spectrum usage efficiency in conventional fixed spectrums gave rise to the Cognitive Radio (CR) concept which came around with the theme of enabling unlicensed access to licensed spectral space for solving the spectrum scarcity issue. First proposed by J. Mitola in

1998, Cognitive radio a promising concept, has risen to totally take advantage of the underutilized spectrum [1]. Spectrum scarcity issue is overcome by allowing utilization of the network resources in the absence of the licensed users by unlicensed users rather than the spectrum resource being wasted (due to absence of the licensed user) thus allowing more number of users to utilize the same resources by adding intelligent usage phenomena to the communicating devices.

Remarkable researches and endeavors have been undertaken on cognitive radios, such as the IEEE 802.22-WRAN [2, 3] and Wireless Innovation Forum (WIF) which includes government regulators, vendors, technology /software developers, academic institutions, research and engineering organizations that support the idea to to take wholesome advantage of "White Spaces" existent in frequency spectrum [4].

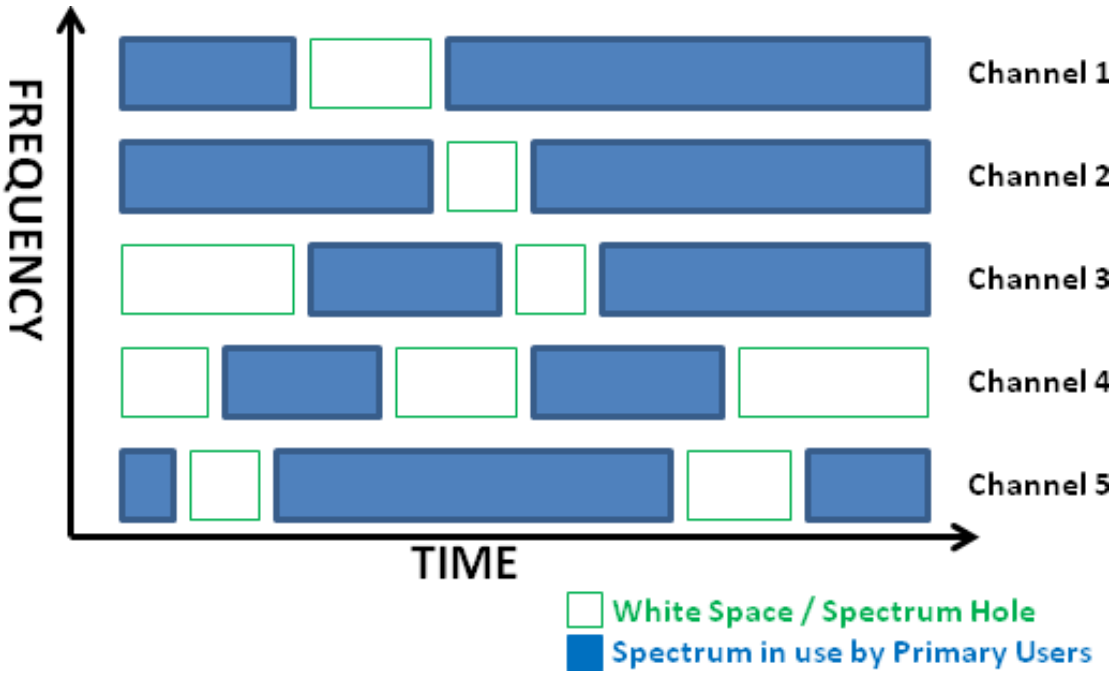

Figure 1.1: White Spaces / Spectrum holes [5]

As depicted in figure 1.1 Spectrum sharing is the general concept of a CR, licensed to primary users (PU) spectrum is leveraged by secondary users (SU) to communicate when PUs are not totally occupying it i.e. vacant space known as "spectrum holes" . SU are required periodically to carry out spectrum sensing utilizing the spectrum in the absence of PU. Whenever the PU becomes active, the SU have to back off

either by reducing transmission power or employ certain time bound vacation [5].

With the surfacing of Cognitive concept in wireless domain many security issues have risen as is the norm with nascent technologies. The inherent attributes of CR paradigm have opened up the gateway to new threats and challenges [6]. If these issues are left on the back burner this may impede all the benefits that can be accrued from this promising technology. There are host of security vulnerabilities to which CRN are vulnerable due to the intrinsic nature of the CR.

1.2 Current Status of Research by Academia

It has been almost two decades since this technology was first proposed and since then Cognitive Radio (opportunistic intelligent utilization of White Spaces) is receiving a lot of importance by the researchers as it is near deployment stage [1]. There is a dire need of better ideas to deploy it in perfect shape. Aforementioned, the Cognitive Radio has a crucial role to play in enabling our wireless conversations of future. Due to many expected contributions, for successful working of Cognitive Radio the likes of coexistence mechanisms, sensing algorithms have been proposed but the security issues received a little less attention.

As far as standardization efforts are concerned a great deal of effort is being made for developing standards related to CRs. Organizations like ITU-R, IEEE and SDR Forum are among the prominent operational in this regard [7, 8]. The most commonly known is IEEE standard, which (relevant to the use of Cognitive Radio) is in the development stage, only draft version of the standard specific to use of Cognitive Radio in TV network (802.22) [2] has been published and the standard relative to use of CRN in CDMA, GSM/GPRS, Wi-Max, LTE and other networks is yet to get any standardization maturity level.

There is no practical application currently in use but as per Federal Communi-

cations Commission (FCC) recommendation the CR technology will be deployed by 2020 in US, therefore companies are finalizing the deployment stages and testing their products to enable their usage [9].

The opportunistic access gives rise to a large attack profile in Cognitive Radio Network (CRN) due to their intrinsic nature. Attacks can be classified rooted on the OSI / TCP/IP layers they impact as covered by authors in [10–12]. However, the papers are piecemeal and fore-go consolidated details and countermeasures about these attacks.

1.3 Motivation

Coginitive Radios (intelligent software defined radios) present a significant area for research vis-a-vis information security; as is with all nascent technologies that they start with a boom and race for technological enhancement and precision sidelining the security issues or totally putting them on a back burner. Since, no system is perfect; hence, capabilities of Cognitive Radio Networks merit that consolidating all known threats, attacks, vulnerabilities and their counter measures is carried out to provide a comprehensive study for future reckoning.

Cognitive Radio (CR) concept came around with the theme of enabling unlicensed access to licensed spectral space for solving the spectrum scarcity issue. Capabilities of Cognitive Radio Networks can be impinged by threats, attacks and vulnerabilities. For spectral resources to be made available/accessible to unlicensed users its utmost important to have a mechanism:

- For discovery of whitespaces in the spectral space for utilization by SU (unlicensed user).
- Which allows no affects of the SU on performance of the PU (licensed user).

What if while sensing some malicious unlicensed user pretends to be a licensed

user?

- Attack can be done by a malicious SU attempting to gain priority over legitimate SUs emanating communication emulating attributes of the PU, thus impinging other SUs from using the network resources [14].

Primary Use Emulation Attack (PUEA) [13] can result in spectrum sensing being critically impinged, reduction in the resources of the available channel to valid Secondary Users (SU), decrease in the bandwidth availability causing connection unreliability and resulting in:

- Quality of Service (QoS) degradation.
- Bandwidth waste.
- Denial of Service (DoS).

PUEA acts as a stepping stone to other attacks such as SSDF attack , Jamming attack, Hello Flood attack, Sink Hole attack etc.

1.3.1 Problem Statement

To elaborate attacks on CRN, many studies have been presented as discussed in previous section. However, the studies focus on identification of attacks on one layer or the other and do not provide a consolidated picture or details of counter measures therefore main motivation was **"to prepare a consolidated reckoner of all types of attacks and their countermeasures"**.

1.4 Objectives

The aim behind the work was to prepare a consolidated reckoner for all types of detection, mitigation and countermeasures vis-a-vis corresponding security threats, attacks,

vulnerabilities to serve as a turnkey solution. Hence, the objectives of thesis work are:

- Elaborating Cognitive Radios (CR) and the Cognitive Radio Network (CRN) with emphasis on working mechanisms, principles, standards and its architecture.
- Consolidating security threats, attacks, vulnerabilities and challenges to Cognitive Radio Networks (CRN).
- Consolidating detection, mitigation and countermeasures against host of different threats, attacks and vulnerabilities to Cognitive Radio Networks (CRN).

1.5 Contributions

1.5.1 Relevance of the Topic to National Needs

Cognitive Radios (CR) as a sub-branch of Software Defined Radios (SDR) are being extensively researched in the entire world. IEEE standard relevant to the use of Cognitive Radio is in the development stage, only draft version of the standard specific to use of cognitive radio in TV network has been published [2] and the standard relative to use of CRN in CDMA, GSM/GPRS, Wi-Max, LTE and other networks is yet to get any standardization maturity level. It is imperative to comprehend this knowledge in stride with the world, as it will usher a new era in licensed spectrum. In harnessing Cognitive based software defined Radios our contribution to international research efforts as a country can also pay dividends. Furthermore, new avenues to securing our software defined radio networks can be looked into.

1.5.2 Relevance of the Topic to Military Needs

Software defined radios utility in the Military cannot be denied. This work would provide a new dimension to ward against SDR/CRN attacks. In future, use of versatile

cognitive radio applications in military cannot be ruled out thus this work would be informative in understanding malicious intents.

1.5.3 Advantages

The research will assist in comprehending the Cognitive Radio based networks. Protection and counter measures against attacks in Cognitive Radio environments.

1.5.4 Areas of Application in Commercial Sector

Contribute to international research efforts in harnessing this technology and securing Cognitive Radio Networks.

1.5.5 Areas of Application in Military

Extensive use of software defined radios in Military merits that attacks, threats and vulnerabilities to SDR/CRN are analyzed. A consolidated reckoner can serve as a turnkey solution to ward against malicious attacks on Military's radio networks.

1.6 Thesis Layout

Divided into six chapters the thesis unfolds as follows:

- Chapter 1: This chapter introduces the topic, describes research objectives and importance of topic to the national needs.
- Chapter 2: This chapter covers setting of the topic in detail. It introduces Cognitive Radios (CR) and Cognitive Radios Network (CRN) working mechanisms, principles, standards and architecture.

- Chapter 3: It provides details of security threats, attacks, vulnerabilities and challenges to Cognitive Radio Networks (CRN).
- Chapter 4: It provides details of detection, mitigation and countermeasures against host of different threats , attacks and vulnerabilities to Cognitive Radio Networks (CRN).
- Chapter 5: This chapter gives an analytical summary of the issues, deployment architecture, attacks and their countermeasures to Cognitive Radio Networks (CRN).
- Chapter 6: This chapter concludes the report.

Chapter 2

FOUNDATION OF CR/CRN

2.1 Overview

Wireless Communications has the highest ratio of deployment/employment amongst all means of electronic communication in the world today; studies suggest that ubiquity of wireless communication has caused a technological explosion. Smart devices as part of IoT, hand-held devices as in PDAs , Tablets, smart-phones, Laptops etc. have made the provision of frequency spectrum an uphill task being exhaustive i.e. usable spectrum has range limits and the range to demand ratio has seen an exponential trend.

The last two decades, Internet utility has rocketed by 1,052 % [15]. This is just one case study, spectrum bandwidth is not utilized by Internet alone ; usage trend of wireless communications means by other technologies is similar to that of Internet. Consider cell phone users for that purpose, the number of users have mushroomed in the last two decades. cell phone services have shifted from legacy networks like AMPS / 2G to more fast networks like 3G and 4G (5G being in the pipeline) meaning more utilization of wireless spectrum resources. This trend would continue in the years ahead. Would there be spectrum bound expansion with usage exponential growth? A simple NO. What does this lead us to then? the necessity of a concept that tackles the expansion of wireless usage around the globe, which is none other than Cognitive Radio.

It is clear that we cannot generate new resources of spectrum all we can do is to use the available spectrum efficiently. Recent surveys performed in the United States show that almost 70% of the allocated spectral resources are idle at some time of the day [15]. Cognitive Radio overcomes the spectrum scarcity issue by allowing utilization of the network resources in the absence of the licensed users to unlicensed users rather than the spectrum resource being wasted (due to absence of the licensed user) thus allowing more number of users to utilize the same resources by adding intelligent usage phenomena to the communicating devices. Provision of opportunistic access is the theme of CR as depicted in figure 2.1 [1].

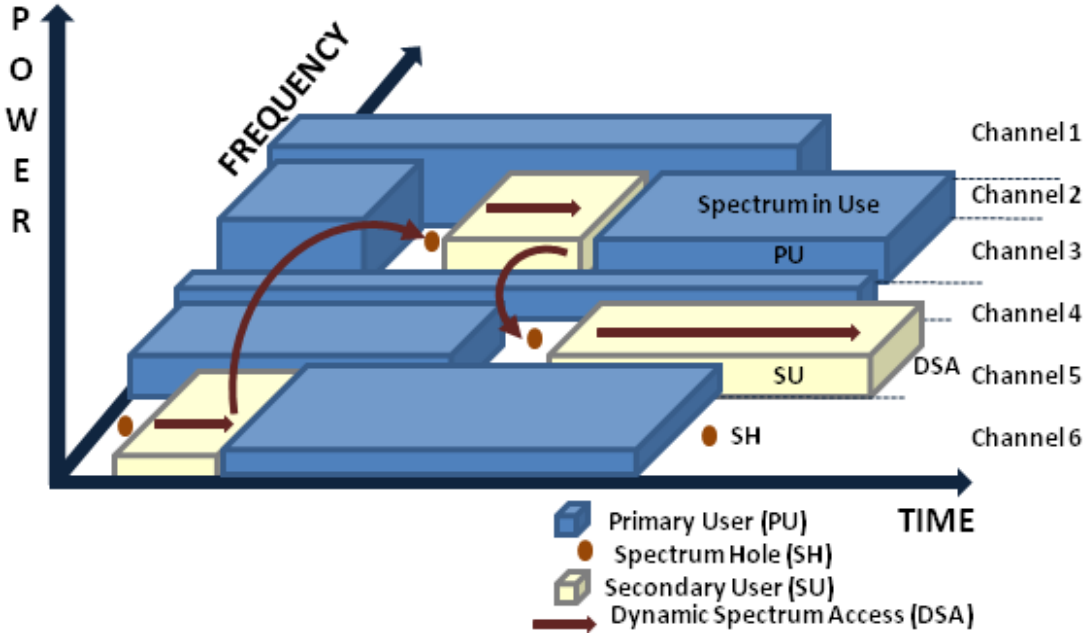

Figure 2.1: Opportunistic Access [1]

The usage of channel by the Secondary User (SU) is bound by the fact that licensed User is away. How would the fact be established ? Sensing is the method employed by SU to check absence of PU from the channel [5]. For spectral resources to be made available/accessible to unlicensed users its utmost important to have a mechanism: For discovery of whitespaces in the spectral space for utilization by SU (unlicensed user) and one which allows no affects of the SU on performance of the PU (licensed user). Former issue is resolved by out-band sensing in the network band-

width based on whose results whitespaces are selected by secondary user depending on its QoS requirements. Once SU selects a whitespace it initiates periodic transmission (with desired SU) and sensing cycle. Hence, two intervals follow each other i.e. sensing (in-band) and then transmission. Hence, in-band sensing by SU resolves the later issue which ensures absence of PU whose whitespace is being currently utilized. SU are required to periodically carry out spectrum sensing utilizing the spectrum in the absence of PU. Whenever the PU becomes active, the SU have to back off either by reducing transmission power or employ certain time bound vacation as in its two seconds via in-band sensing for IEEE 802.22 standard [5]. The two-interval cycle of sensing and transmission by SU continues until communication is completed or emergence of PU.

2.2 The Vision of CR

Vision that led to development of this promising technology was to have a system that detects and utilizes the bandwidth more systematically and productively. If the spectral resources are to be utilized as stated in the previous section then this will lead a user to find the available resource in spectrum which may add time as an overhead. By learning the domain conditions CR can enhance link consistency and aid NWs to automatically boost capacity as well as coverage [16].

2.3 Advantages of CR

Use of Cognitive Radio as discussed in the previous sections will make the networks inter-operable allowing them to communicate with different protocols. Interoperability will increase the coverage and data rate considerably making the global roaming easier. This technology would also allow us to overcome the drawbacks of the legacy analogue components. Types of switching to communicate over any network are:

- Packet Switching: In packet switched networks the resources are shared among users
- Circuit switching: In circuit switching networks the resources are reserved and hence wasted.

A lot of spectral resources can be saved using CR which involves packet switching preeminent [17].

2.4 CR

Definition : *"CR is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding by- building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind: highly reliable communication whenever and wherever needed; efficient utilization of the radio spectrum"*[18]

2.5 Cognitive Cycle

The concept behind Cognitive Radio can be best understood by looking at cognitive process itself [19]. As depicted in Figure 2.2, it consists basically of four steps:

1. Sensing.
2. Analysis & Reasoning.
3. Adaptation.
4. Acting.

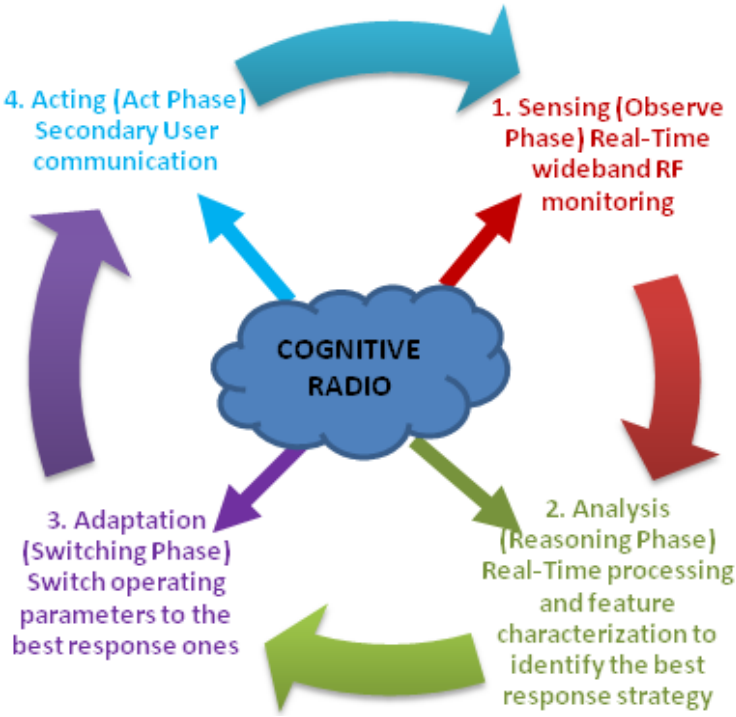

Figure 2.2: Cognitive Cycle of CR [20]

Sensing is performed first and it is the most important step involved in this cycle. Based on the sensing results the radio performs analysis of the sensed data as per its QoS requirements or in other words the results are analyzed and characterization of the environment is done as per the QoS requirements. When the analysis has been performed, reasoning is performed based on type of radio. In case of policy radio the reason to adapt to new parameters comes from the hard coded policies where as in learning radio it is the AI engine that helps gathering the reasoning to perform adaptation. All the succeeding actions performed in the cognitive cycle are based solely on the sensing results. In the end adaptation is performed to make a transition to the new operating parameters. Finally,Acting i.e. secondary User communication starts.

2.5.1 Tasks performed by the CR

Complying the cycle discussed in the previous section, the CR performs the following:

- Radio analysis

- Channel identification
- Dynamic spectrum management.

Radio analysis is done to avoid any interference limit and to detect presence of white spaces. Channel identification is performed to achieve coherent detection and it will also enhance the spectrum utilization. Dynamic spectrum management is also performed at the transmitter to take decisions ensuing from the outcome of preceding actions [21]. The tasks can be summarized as depicted in the Figure 2.3.

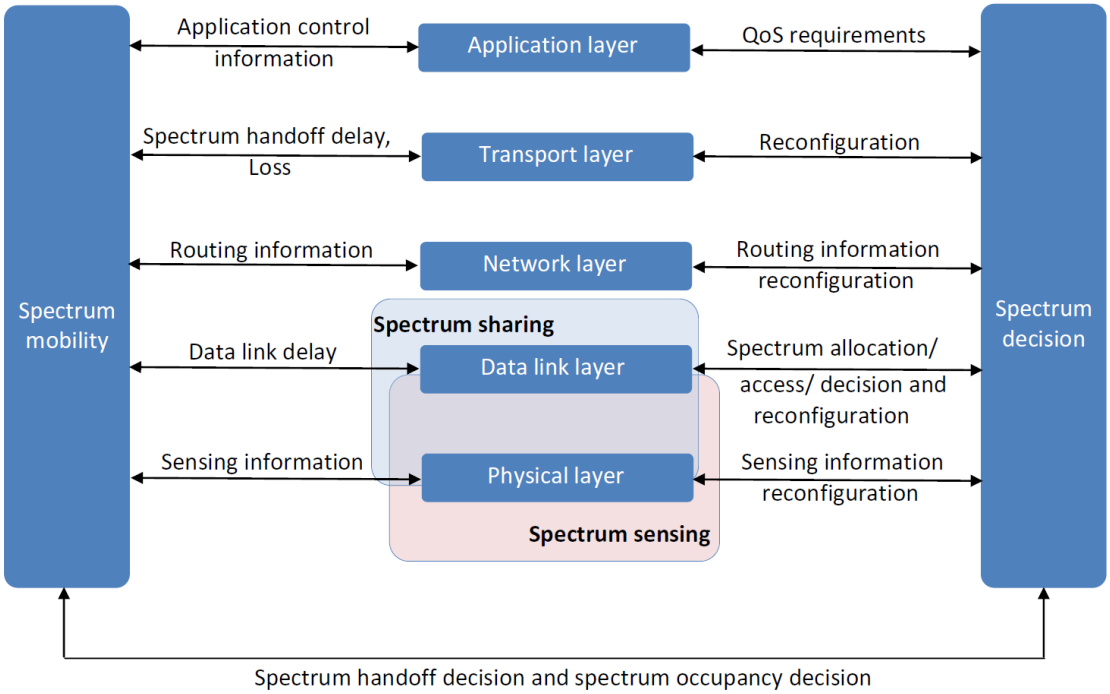

Figure 2.3: Spectrum Management Tasks [22]

2.5.1.1 Transmit Power Control / Dynamic Spectrum Management

Towards end when the available spectrum range has been known the CR will choose the criteria such as the vacant spaces and level of power to transmit. In this case managing the spectrum would make the following possible [17]:

- SU utilizing the vacant spectrum has to coexist with the PU.

- Interference must not surpass a certain set level.

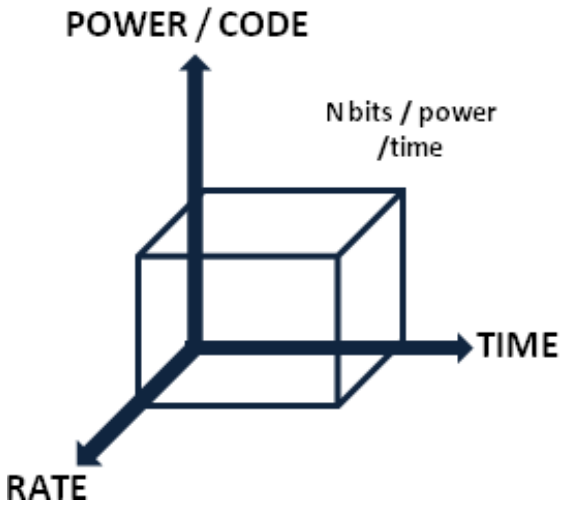

Figure 2.4: Power Rate - Bit Rate

Power/ bit rate control as depicted in figure 2.4 and spectrum management is all done at the transmitter end. Another important attribute here is the transmission technique, which mainly fall into the following categories:

2.5.1.1.1 Overlay This transmission technique allows parallel transmission of the PUs and the SUs, this procedure is also known as the concurrent transmission. The SU uses part of its power for its own transmission and some part to relay the PU data as depicted in figure 2.5.

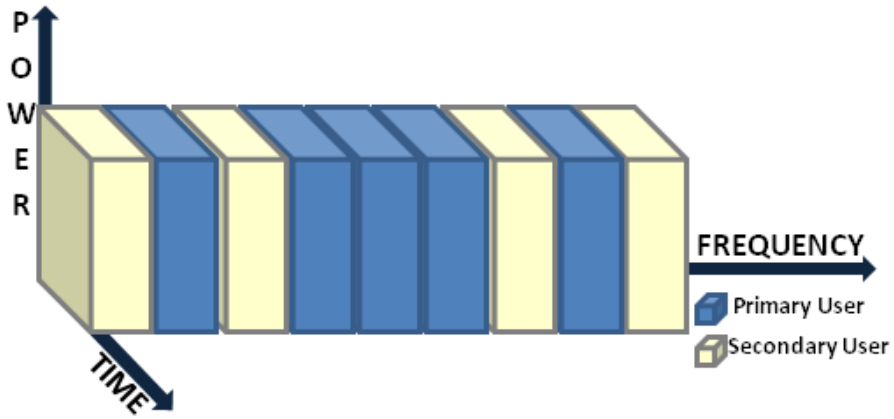

Figure 2.5: Overlay

2.5.1.1.2 Underlay This allows concurrent transmission or parallel transmission of the PU and the SU in the Ultra Wide Band. But due to power issues underlay scheme provides short range of communications. The difference between overlay and underlay is that underlay is limited to short range communications as depicted in figure 2.6.

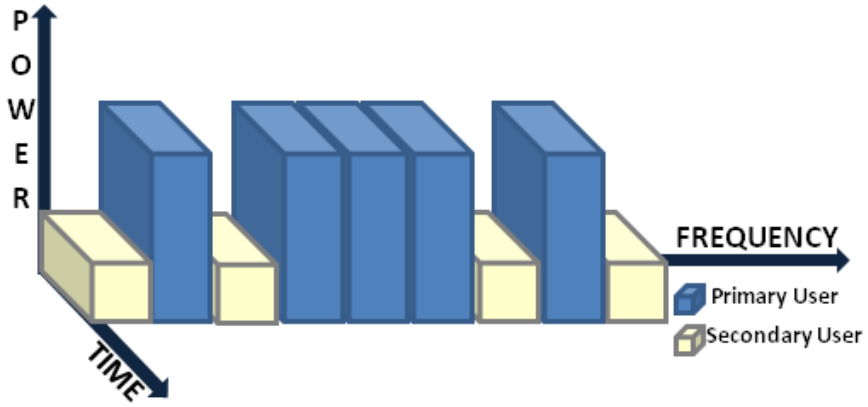

Figure 2.6: Underlay

2.5.1.1.3 Interweave Here the CR will monitor the spectrum from time to time and then communicates over the available vacant spectrum regions. It will communicate in such a way that whenever the PU will communicate the SU will remain silent in that particular band [23].

2.6 CRN Architecture

Deploymnet of CRNs can be in three different ways i.e. the architecture can be : centralized, distributed and mesh [24].

2.6.1 Centralized

Infrastructure based: CRN infrastructure based architecture is depicted in Figure 2.7, which is a centralized approach and access to a base station (BS)/ fusion centre (FC) by an SU can only be in one hop. BS shall control all communication amongst SU which

are in its transmission range. Backbone is through which routing of communication amongst different cells occurs. BS receives sensing information from the SU periodically. The BS/FC aggregates this information collected from different SU to take the decision based on which operating parameters are reconfigured by the SUs [24].

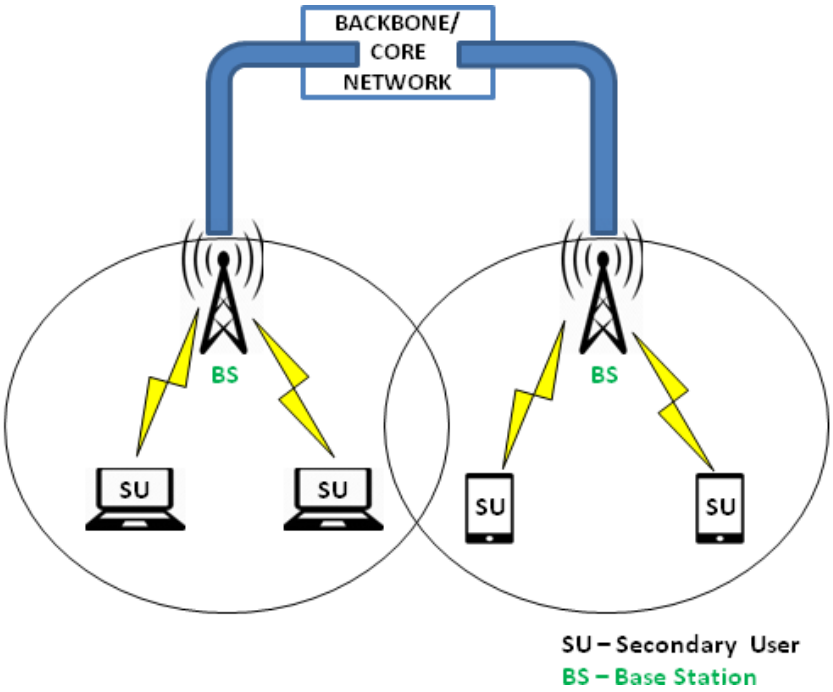

Figure 2.7: Infrastructure Architecture [24]

2.6.2 Distributed

Ad-hoc: Figure 2.8 shows CRN Ad-hoc based architecture which is a de-centralized approach and does not rely on any predefined infrastructure. On emergence of an SU in transmission zone of another SU, a link may be set up resulting in formation of an ad-hoc network. Hence, two or more SUs can either communicate with each other by dynamically utilizing the white spaces or across prevalent communication protocols/standards(e.g., WiFi, Bluetooth). In absence of a central coordinating authority, the SU must rely on local coordination i.e. amongst thems to gather topology information and to conduct communication [24].

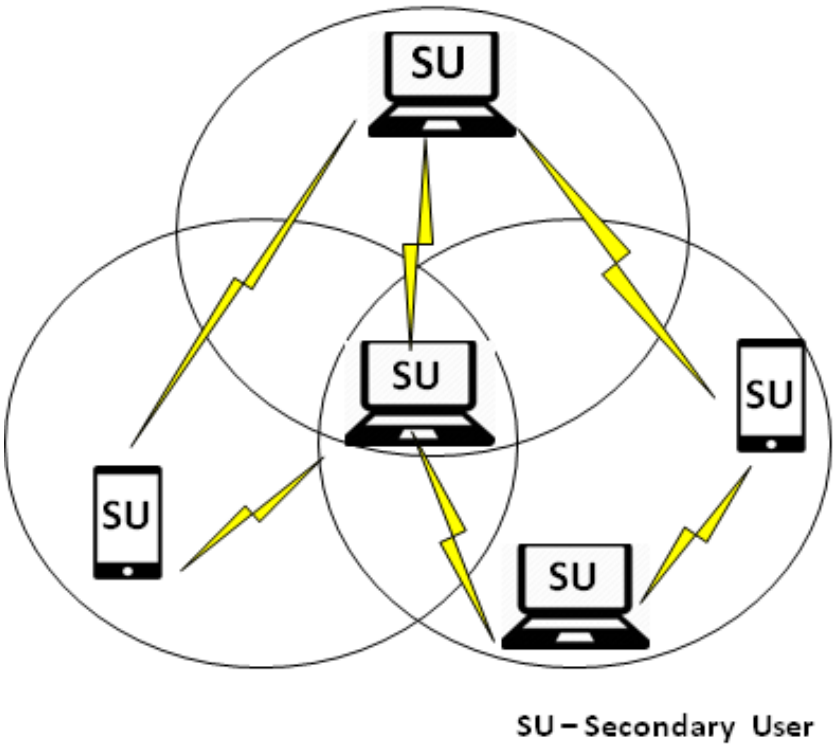

Figure 2.8: Distributed Architecture [24]

2.6.3 Mesh

Figure 2.9 shows CRN mesh architecture a combination of both of the previous stated architectures facilitating the communication between BS to BS, BS to SU and SU to SU. The wireless backbone is formed by BS working as wireless routers. SU can directly connect to the BS or through relay nodes i.e. employing other SU in a multi-hop process. Connectivity to wired backbone or core networks may also be carried out by some BS which may function as gateways [24]. Spectrum holes can be utilized by BS having cognitive radio capabilities to communicate each other as well.

2.7 Implementation Issues

The initiation and development of this promising technology presents many challenges. Following are the implementation issues that pose a challenge to deployment of CR [19, 21]:

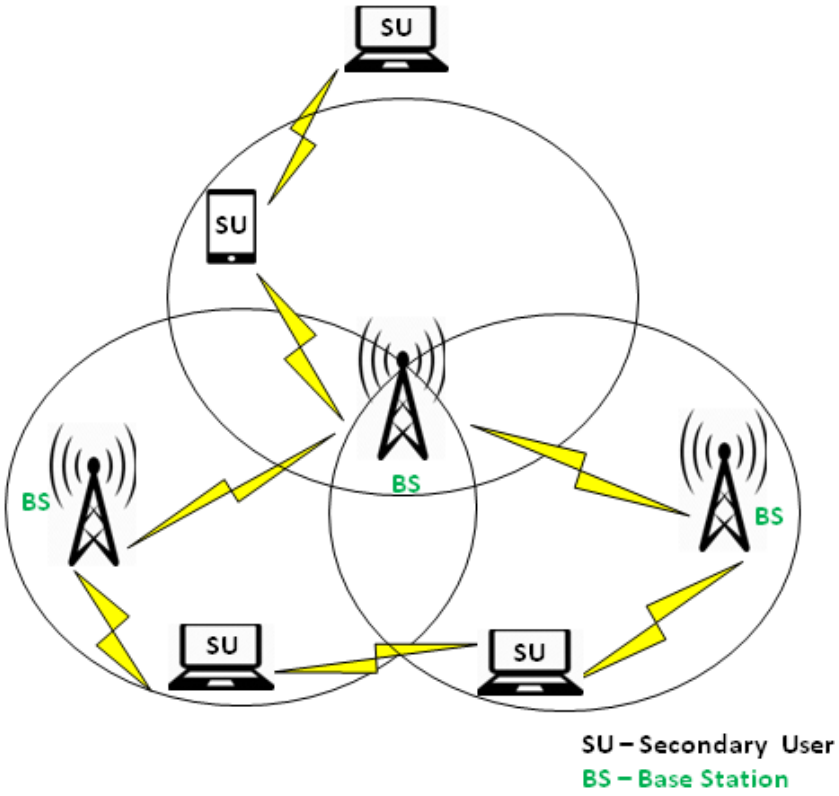

Figure 2.9: Mesh Architecture [24]

1. Sensing [25, 26].

2. Interference Management [27].

3. Resource allocation [27].

4. Architecture.

5. Physical Layer.

6. Protocols and Standardization [2, 29].

7. Signaling.

8. Security.

2.7.1 Sensing

This is the most important characteristics of the CR. The CR must have to ability to sense the radio channel, or in other words the CR must have ability to know when the spectrum is available and at the same time sensing is important to ensure non-interference with the PU because it is sensing that lets the SU know that the PU has reappeared. Two types of sensing is performed by the SU:

1. **Out-band sensing**: To search for white spaces or vacant holes in spectrum.
2. **In-band sensing**: This is periodically carried out by the SU once white space utilization is started by the SU. This ensures non-interference of the SU on performance of the PU.

There are three kinds of spaces that exist in the spectrum which sensing takes into account:

1. **Black Spaces**: Spaces engaged by devices with high power interference
2. **Grey Spaces**: Grey Spaces are employed by devices with little power interference.
3. **White Spaces**: White Spaces are free to use.

Black spaces are forbidden to be used by the SU for transmission because of the high power interference. So the concerning are white spaces and grey spaces. Spectrum sensing can also be termed as spectrum detection because sensing involves detection; many schemes were proposed to identify the white spaces in the spectrum, sensing techniques are mainly of two types [25]:

2.7.2 Security

More research carried out till now is focused towards other issues, but unfortunately the security issue gathered a little less attention as compared to other issues. Security is the most critical aspect involved in the implementation of CRN, because if an attack (due to an unaddressed security issue) occurs, then CR will be unable to deliver its basic functionality that is the opportunistic access.

Work needs to be done on developing secure protocols for the SU having mechanism such as authentication, authorization. CRN is based on the premise that PU and SU are to be differentiated in the network, authenticating PU and SU is specifically mandatory since both PU and SU deserve different level of authorization and different privileges to access the spectrum. Authentication can be easily implemented for centralized architectures by having a centralized authority; however it is difficult to implement such scheme in a distributed/ non-cooperative environment.

The CRN provides conditional authorization. Conditional authorization refer to the term where the SU can only transmit in licensed frequency bands till the time the Primary User for that licensed band does not require that band.

In the following chapter security issues to CRN by describing possible attacks, threats and vulnerabilities will be described.

Summary

Details about CR were discussed. Firstly the need that became the reason for invention of CR was discussed and then the importance of CR in solving the spectrum shortage problem was discussed. In the following section the Cognitive Cycle was introduced and described. Then discussion was made on tasks performed by the CR including analysis, channel identification and spectrum management.Then CRN architecture was described. In the last section issues related to deployment of CR were listed .

Chapter 3

SECURITY CHALLENGES

3.1 Security Threats

With the improvements in technology, security based threats also emerged on the horizon that would serve as a impediment to the advantages these innovations bring along. Each node which is part of a network is susceptible to many security based threats. The threats are not only limited to nodes of existing technologies but these threats pose serious challenge to upcoming technologies like Cognitive Radio. As far as standardization efforts are concerned a great deal of effort is being made for developing standards related to CRs. There is no practical application currently in use but companies are finalizing the deployment stages and testing their products to enable their usage [9]. There is a dire need of better ideas to deploy it in perfect shape. Cognitive Radio solves spectrum paucity issue; moreover, it would have amplified utility in numerous applications once it gets deployed, consequently it is vulnerable to many attacks. Attacks to CR are discussed in detail in this chapter.

The attack profile is quite diverse in cognitive radio networks due to their intrinsic nature, attacks can be classified according to the layers they impact as portrayed in Table 3.1: Application layer, Transport layer, Network layer, Link layer/ MAC, Physical layer and Cross layer.

Table 3.1: Attack Profile - Protocol Layers

Layer		Attacks	
Cross layer	Application layer	MW	CAA; RIJ; SBW; JFA; LION
	Transport layer	KDA	
	Network layer	Sinkhole; Wormhole; HELLO; Sybil	
	Link layer/ MAC layer	SSDF; CCS; CCC	
	Physical layer	Jamming; OFA; PUEA; OSU	

3.1.1 Application layer

The layer which represents the control panel / Graphic User Interface (GUI) that is physically visble to the user and near proximity of the user. Operator through the end user-program / Software (SW) interacts with this layer. Identification of communicating devices, synchronizing communication and making resources available are few of the functionalities at this layer. CR continous spectrum sensing and learning process makes the memory and CPU power requirements far greater than the conventional hand held devices. CR are expected to be targeted by Malware (MW) / Viruses [30]. Moreover, Transport layer frequent key exchanges, Network layer routing issues, Link layer/ MAC layer & Physical layer spectrum handoff issues cause deterioration of services at this layer in short the QoS is affected [31].

3.1.1.1 MW

"*Malware*" : The CRN is as exposed to malicious software/ programs as any other software defined NW i.e. NW managed through SW. MW (viruses, worms, Trojans) are computer programs that can proliferate from device to device through exponential multiplication and self propagation. In a self propagating NW like the CRN, MW can be extremely destructive. A CR corrupted by MW can transmit false data and carryout all types of attacks possible in the layers below. MW will impact the whole **Cognitive Cycle of CR** [20] sensing, analysis, adaptation and acting pushing it to react / act to the false variables and parameters, affecting future NW decisions.

A self propagating MW Proliferation model through a CRN has been presented in [32], with details of how MW impacts CRN. It starts with emphasis on time; foremost, Time taken to infect the CRN increased exponentially with network size. Furthermore, how in static NW the antivirus (AV) performance is better than mobile dynamic NW. Finally, Propagation speed of MW increases with abundant spectrum resource.

3.1.2 Transport layer

CRN face the same issues at this layer faced by classic wireless communication [33].

3.1.2.1 KDA

"*Key Depletion Attack*" : CRN transport layer sessions duration are short due to excessive return trip phase and periodic recurrent transmissions [30]. Hence, applications generate substantial number of sessions. Security protocols at this layer like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) initiate cryptographic keys at the inception of every single session. The keys are generated through a pseudo random number generator (PRNG) which is eventually exhaustive and with substantial number of sessions at hand the probability of a key being repeated twice increases. Repetiton

of any key increases the chances of its exposure which can resultantly compromise the whole cipher system.

3.1.3 Network layer

CRN Mesh, Distributed(ad-hoc) and Centralized architectures face the same issues at this layer faced by classic wireless communication [33]. CRN and wireless sensor networks (WSN) share many similarities with each other which include power constraints and multi-hop routing. Routing in the CRN is complicated by the fact that the SU has to quit the frequency every time the PU presence is sensed.

3.1.3.1 Sinkhole

Sinkhole attack is done by an MU who publicizes itself as the shortest cost effective path to a particular target in multi-hop routing, persuading neighboring SU to use it for forwarding their packets [34]. As the MU receives packets from all SU, it can either read the conversation or drop the packets by not forwarding it to the destination it was meant for. A severe form of this attack is where MU advertises itself as best path to the base station in case of Centralized schemes as shown in figure 3.1.

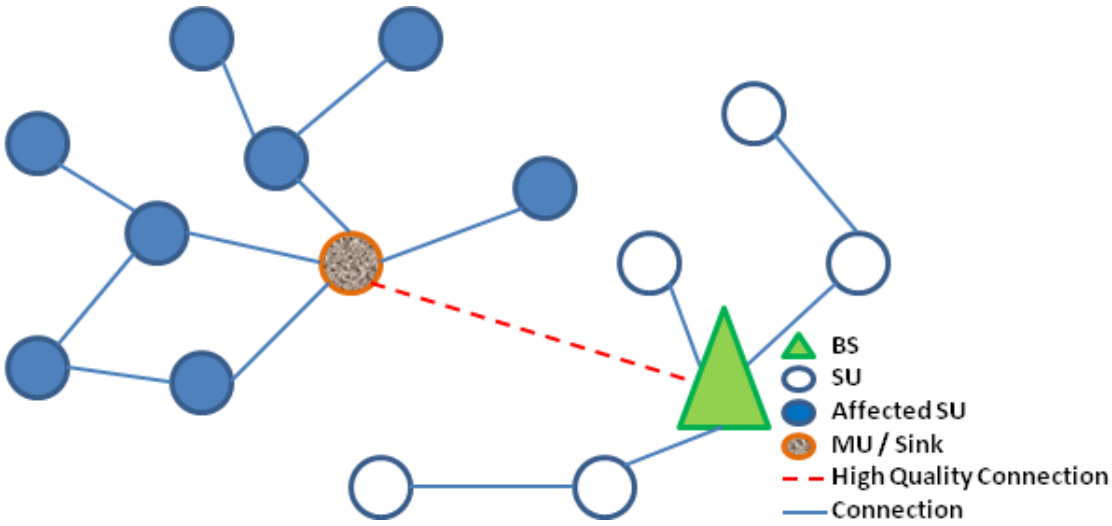

Figure 3.1: Sinkhole Attack [34]

3.1.3.2 Wormhole

Wormhole attack and Sinkhole attack are closely related to each other. The origin point i.e. MU relays packet to the destination point i.e. sink node as shown in figure 3.2. The MU and sink node administer wormhole attacks by understating the route amongst themselves and the BS and then transmitting data through the channel that is barred to the other nodes [33]. Basically, MU *"tunnels"* packets acquired in one part of the NW over a connection with meager delay to the sink in the NW which are then replayed into the network from that point.

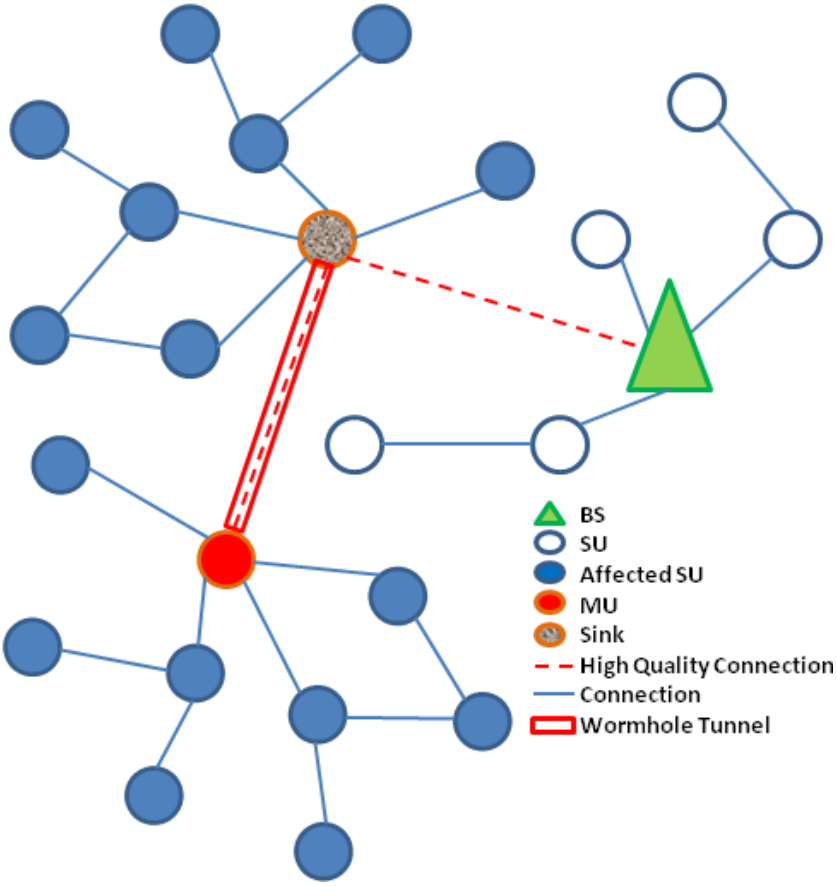

Figure 3.2: Wormhole Attack [33]

3.1.3.3 HELLO

HELLO attack is done when a MU broadcasts a packet to all nodes in a CRN, with sufficient transmission power to persuade them that the MU is their neighbour [33]. A MU may use this attack from far away to convince the victim that he is their neighbour as shown in figure 3.3. As a result of this victim switches to wrong route and does all its transmission through the MU. This will result in high number of lost packets. Since all of them will be using the same route, even if the victim realizes it, it would have no alternate route available to forward its data as all the co-existing neighboring nodes are under the same spell and they would be forwarding their data/ packets to the MU as well.

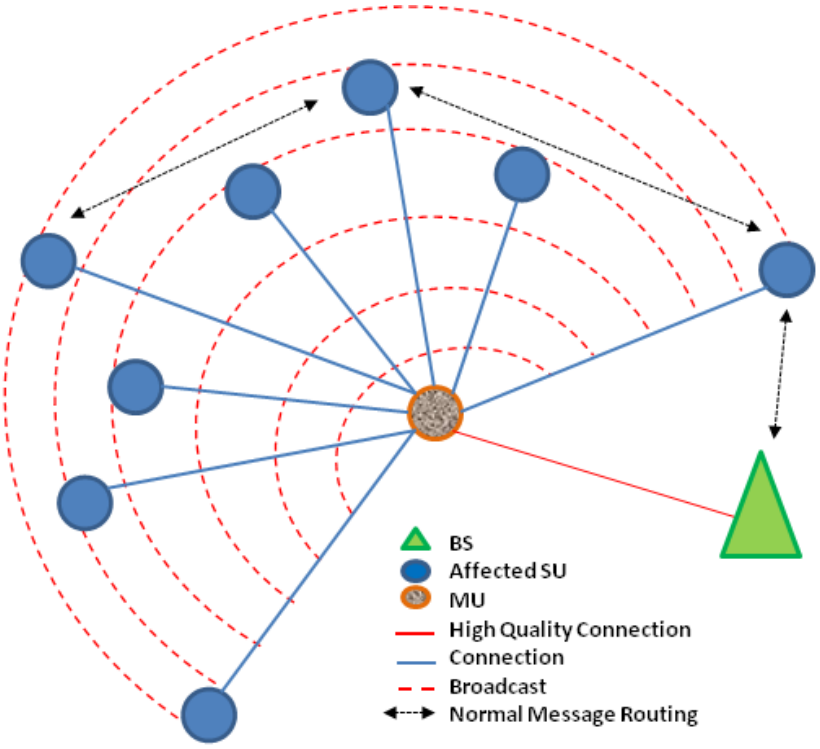

Figure 3.3: HELLO Attack [33]

3.1.3.4 Sybil

In Sybil attack a MU masquerades several distinct SU by requesting spectrum with distinct fake identities which is done by transmitting beacon frames inserted with disparate identity data to co-existing SU as shown in figure 3.4 [35, 36]. This misleads other SU to believe in each identity being broadcast by the MU as a legitimate SU and this attacks further association with other types of attacks causes significant vulnerability. Analysis of the vulnerability of Sybil-based PUEA and SSDF in DSA network has been carried out [10].

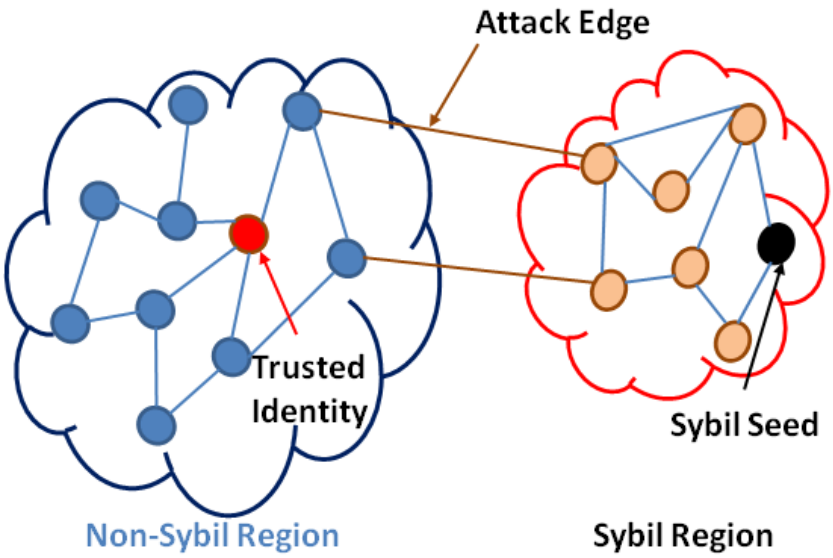

Figure 3.4: Sybil Attack [36]

3.1.4 Link layer

The attacks are mainly collision based.

3.1.4.1 SSDF

"*Spectrum Sensing Data Falsification*" / *Byzantine attack* : SSDF is done by an assailant who is a legitimate member (Byzantine [10]), by sending incorrect spectrum sensing results to its neighbors (in case of Distributed schemes) or to the BS/ FC (in case of cooperative Centralized schemes) as shown in figure 3.5. This propagation of false sensing results to the neighbours causes a wrong spectrum-sensing decision at the victim [31, 33]. The intent can be selfish or malicious. Both Centralized and Distributed CRN are susceptible to this attack. SSDF is highly destructive in Distributed CRN, for the reason that incorrect data spreads rapidly and there is no mean to restrict its spread, however, in the Centralized CRN, the central entity can reduce the impact of incorrect data by matching the information acquired from all nodes in CRN.

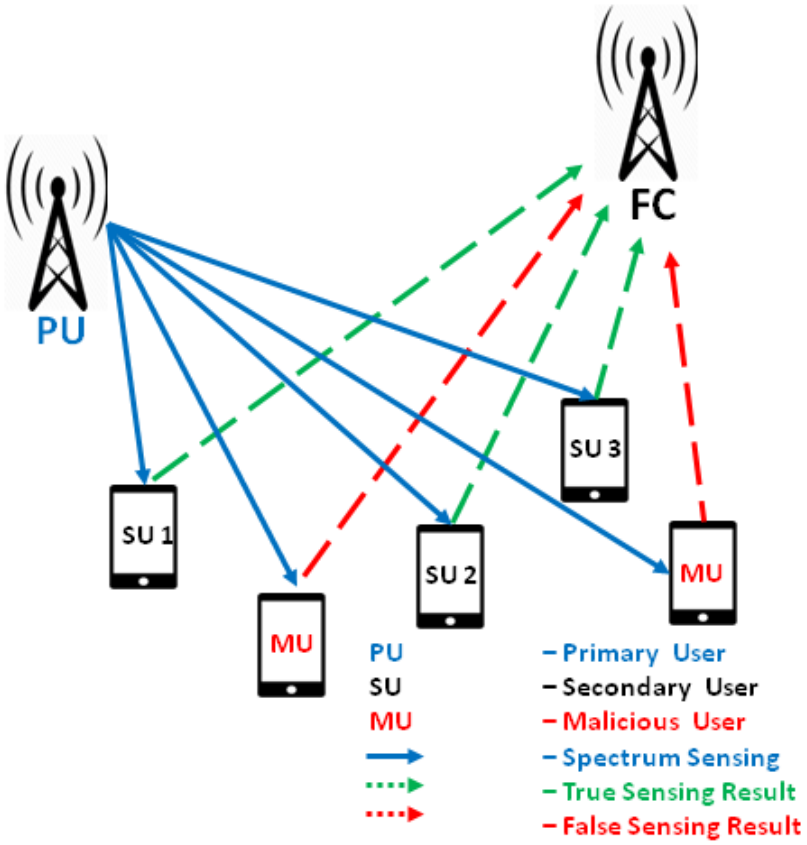

Figure 3.5: SSDF Attack [31]

3.1.4.2 CCS

"*Control channel saturation*" : In a CRN with multiple nodes, the nodes perform channel negotiation in Distributed manner, prior to their communication. During the channel negotiation several control frames are swapped to book the channel. Since numerous nodes may want to transmit simultaneously, therefore CC used for exchanging control frames may become a bottleneck due to finite capacity of the control channel. An attacker intending control channel saturation DoS attack may generate fake control frames to occupy the CC and consequently degrade the NW capacity through collisions [37]. It is significant to mention here that this attack is applicable only to Distributed CRN because all control frames in Centralized CRN are passed after authentication by the central entity. This attack can be selfish or malicious. With the combinaton of the small window backoff attack(SBW) and control channel saturation (CCS) attack the MU (agressor) seizes the CCC before other users.

3.1.4.3 CCC

"*Common Control Channel jamming*" : Cooperation is facilitated amongst nodes in CRN through "*Common Control Channel*" (CCC). CCC jamming is the extremely energy efficient & effective technique for a malicious user to block the entire CRN [38]. Through injection of a strong signal into the CCC, receivers are prohibited from valid control messages. This results in DoS for nodes of the CRN.

3.1.5 Physical layer

Dynamic Spectrum Access (DSA) makes the operation of CRN quite complex.

3.1.5.1 Jamming

Jamming in other words can be termed as a Interruption / DoS attack. The attacker in this attack creates a situation where the legitimate SUs cannot send or receive data by affecting the signal to noise (SNR) ratio. Such situation can be created in different ways such as sending continuous data packets so that the legitimate SU never finds channel idle as shown in figure 3.6. In another technique the attacker may send continuous packets to receiver thus making it unavailable by occupying all the communication capacity that it has or in other words creating a ping to death.

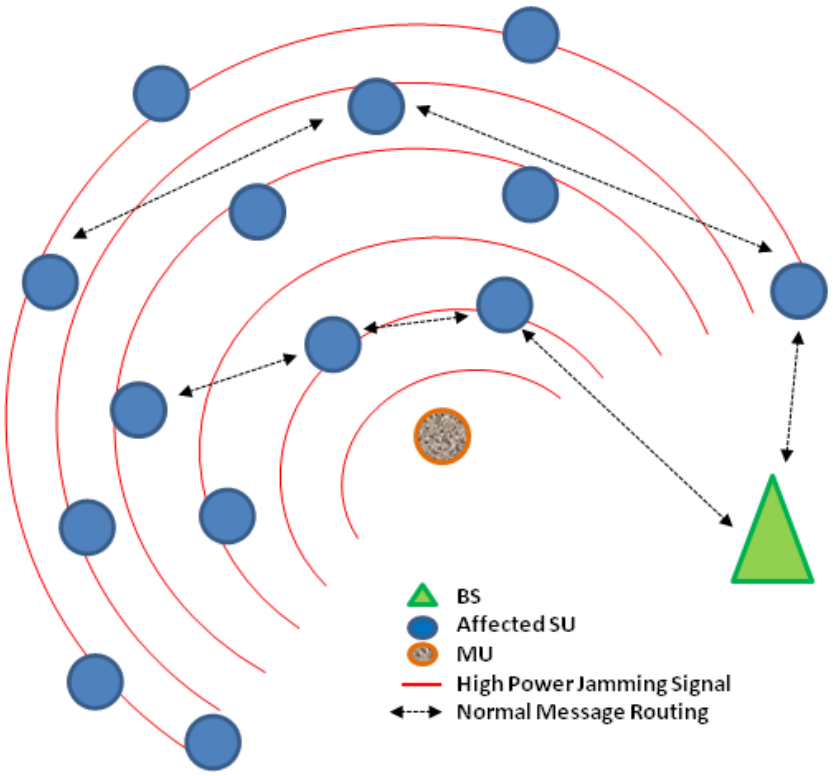

Figure 3.6: Jamming

In yet another technique the attacker may use the methodology of smart jamming in which the attacker uses the information of the learning radio instead of transmitting continuous packets and comes into action when the victim radio tries out transmission.

To make things even more worst the attacker may disrupt communication that would result in the distortion and deformity of packets being transported to genuine

SUs. A further hazardous knockout may occur in cooperative (Mesh) schemes of CR where the intruder jams the channel dedicated for exchange of sensing information between CRs.

Jamming attack can be done on the data link and physical layers. Jammers can be categorized as follows:

3.1.5.1.1 Reactive jammer Employs continuous sensing of channel all times and whenever it detects any communication, jamming signal transmission begins. Since, transmission is not continuous consequently the jammer is solider to identify/ spot.

3.1.5.1.2 Deceptive jammer Works by deceiving authorized users by ensuring they switch into reception by transmitting constant continuous high power communication.

3.1.5.1.3 Constant jammer Transmits data packets uninterruptedly with archaic disregard to the data link layer protocols.

3.1.5.1.4 Random jammer Inserts quite intervals between the jamming signals, however it adopts the behavior of a constant or deceptive jammer. The reason of inserting quite intervals is to conserve energy.

To accomplish this attack at the *physical layer*, the aggressor may employ a specialized gadget such as programmable radios and waveform generators, adept at emanating power in sync with frequency employed by nodes in the network. This creates interference among the transmissions.

Sampath et al., in [39] illustrates an attack layout where a lone CR sends jamming packets to multiple channels. It sends packet to one channel and switches through channels quickly after it has sent the desired number of packets. This process repeats and after the last channel has been struck, the aggressor returns to the already targeted

channels and repeats the jamming cycle.

To perform this attack at *Link layer*, the attacker sends attack packets to a particular radio channel, thus creating a situation where all nodes in the radio vicinity start assuming the presence of a legitimate user and engagement of channel. Hence, delaying their transmission as described in [40].

3.1.5.2 OFA

"*Objective function attack*" : The CR is basically a smart SDR that observes its environment and adjusts accordingly. The cognitive engine is responsible for adapting according to the certain parameter such as channel access protocol, coding rate, modulation type, power, bandwidth etc., in order to abide by the obligations such as high security, high data rate and low energy consumption [41]. The cognitive engine which has the sole responsibility for all this calculates these parameters by unraveling the objective functions. The attack done on a CR cognitive engine when the cognitive engine is running and resolving the objective functions so as to find the appropriate radio parameters to adjust to according to the current environment is called Objective Function Attack also known as *"Belief Manipulation Attack"*. The intent behind this attack is that attacker can make the results such as channel access protocol, frequency, modulation, bandwidth etc. tailored according to his interest.

3.1.5.3 PUEA

"*Primary User Emulation attack*" : CRN has to distinguish between the PU and SU. In the PUE attack, a malicious node/user (MU) modifies the access mode by emulating the PU signal attributes making other SU believe that the band is employed by the licensed user, and so making other SU to step aside or vacate the frequency as shown in figure

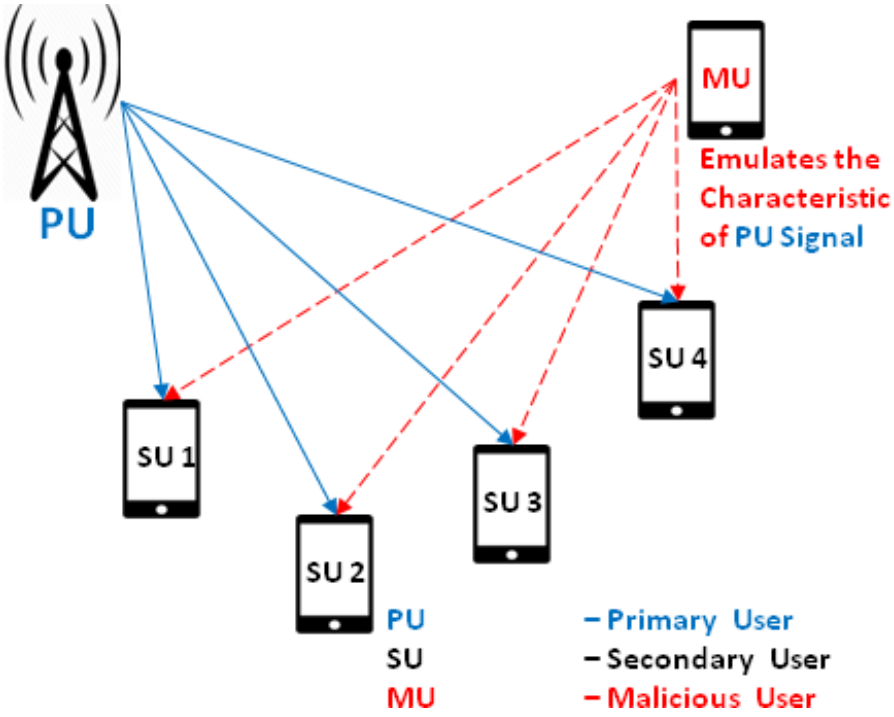

Figure 3.7: PUE Scenario [13]

3.7 [13]. The objective of the impostor could be selfish or malicious; in any case the result is a DoS attack [14]. Hence, the primary user emulation attack (PUEA) can be said to lead to OFA .

3.1.5.4 OSU

"*Overlapping secondary user*" : Overlapping secondary user (OSU) are present at the boundary of two or more overlapping coexisting networks as shown in figure 3.8. Now this OSU intentionally or unintentionally can affect the objective function or the PUE vulnerabilities thereby placing the DSA sharing at risk. OSU may broadcast transmissions that may impair the PU and SU of the overlapping coexistent networks by impinging their objective function (a kind of OFA in the making as well) through erroneous sensing data [37, 42] or emulation as a PU thereby causing the vacation of channel by the overlapping networks.

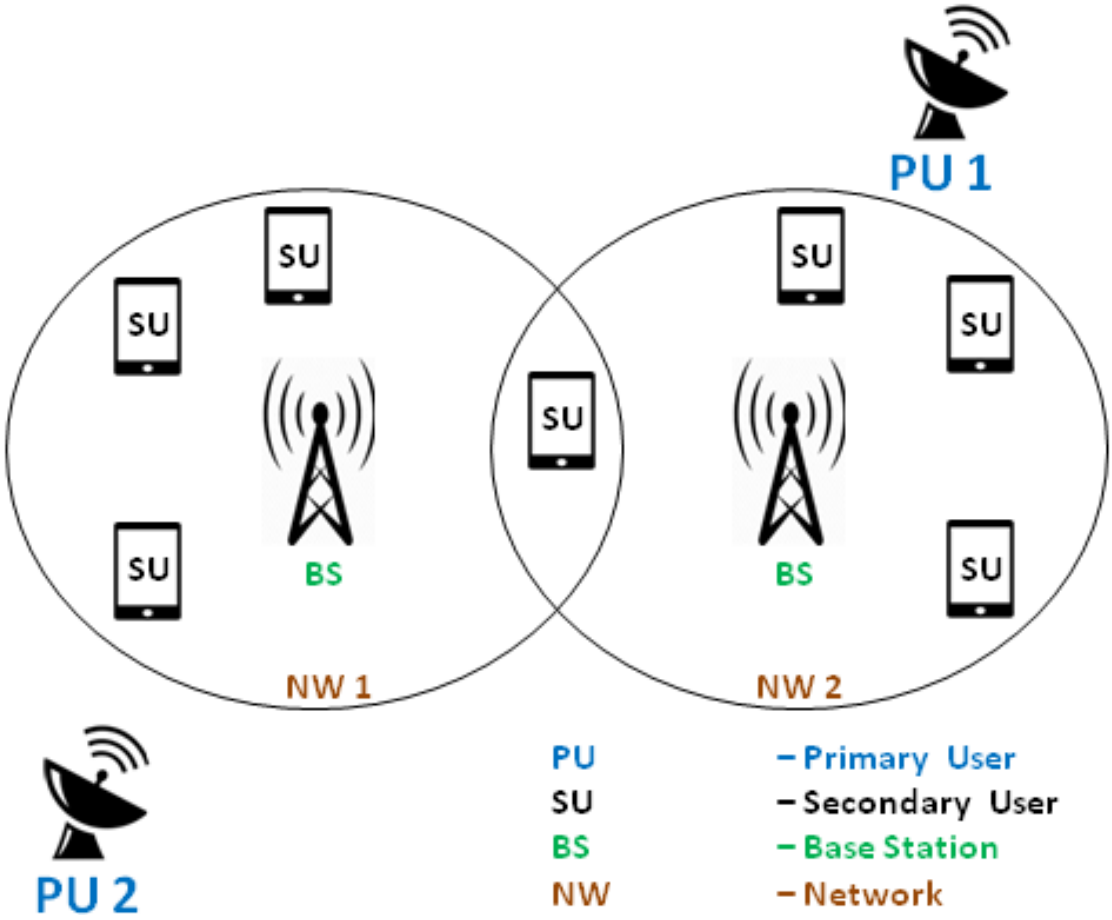

Figure 3.8: OSU Scenario [42]

3.1.6 Cross layer

"*Cross-layer attacks*" are targeted across multiple layers and impact the whole **Cognitive Cycle of CR** [20] . A combination of those enlisted in Table 3.1 can be used to create these attacks. Furthermore, intrusion targeting one layer may impact performance at others by re-initializing **Cognitive Cycle of CR** [20] repeatedly. Often these attacks are directed towards Physical layer but their affects propagate to the Link layer and beyond.

3.1.6.1 CAA

"*Channel assignment attacks*" : DSA is critical to increase the throughput of the CRN

to avoid interference and ensure the optimal channel usage [43]. CAA is more applicable in Mesh and Distributed CRN as compared to Centralized, as they are collaborative architectures based on multi-hop routing alogorithms. DSA algorithms are vulnerable to numerous attacks [44] such as "*low-cost ripple effect attack*" (LCRA), "*channel ecto-parasite attack*" (CEPA) and "*network endo-parasite attack*" (NEPA). CEPA and NEPA aims to increase the interference at heavily loaded high priority channels. A MU in NEPA after assigning high priority bands to its access modes does not transmit the change data so that other SU remain aloof. CEPA is a subset of NEPA in which MU targets all the channels using the highest priority link by switching all its interfaces to them, its serious impact on the network makes it easy to detect. MU in LCRA affects the **Cognitive Cycle of CR** [20] by transmitting misleading channel assignment (CA) information to other SU and resultantly the SU adjust their CA this leads to generation of series of changes in CA in the multi-hop environment because of transmission of this falsified information hop by hop throughout the network . This propagation of change has a crippling effect as compared to CEPA & NEPA because of the spread to the larger portion of the network beyond immediate SU.

3.1.6.2 RIJ

"*Routing information jamming*" : CR with no CCC are vulnerable to this attack. During spectrum handoff there is delay. This delay resultantly enables interruption / denial of the routing data among SU. The ramification is incorrect routing using prohibitive routes. Before the information regarding routes is exchanged MU prompts the ear marked SU to commence spectrum handoff. When this transpires, the assailed SU halts entire current transmission and carries out the **Cognitive Cycle of CR** [20] anew. Until the handoff is complete the SU cannot transmit or receive updated routing information known as *"Deafness"*. The MU can extend the attack and make it more severe by continuously forcing spectrum handoff just before routing information exchange [31].

3.1.6.3 SBW

"*Small Backoff Window*" : SU are required to periodically carryout spectrum sensing to discover the existence of **White Spaces / Spectrum holes** [5]. In the eventuality of sensing the channel to be occupied the SU backs off for a random time. This randomness is used to minimise the probability of collision between SU trying to access the channel. When the channel is idle the random back off window size is decremented and when the chanel is occupied it is doubled before re-sensing again. A MU can *"selfishly"* decrease the back-off window size to gain priority on channel access over other SU this behaviour is called back off manipulation or SBW attack which can severely impact the throughput of the whole CRN [45].

3.1.6.4 JFA

"*Jelly fish Attack*" : This attack is a DoS that's carried out at Network layer by MU but repercussions are faced at the Transport layer particularly effecting the performance of the Transport Control Protocol (TCP) [31]. Attack by MU at the Network layer affects multiple layers [45]. Intentional delay of data packets by MU is carried out before transmission and reception in the NW. MU may also distort the order/sequence of the data packets it receives and transmits to affect re-assembly thereby degrading the performance of the NW. JFA is categorised as "*jellyfish recorded attack*", "*jellyfish periodic dropping attack*" and "*jellyfish delay variance attack*" [46].

3.1.6.5 LION

LION Attack : is carried out at the Network layer resultantly exploiting instinctive capability of TCP at the Transport layer. The PUEA forms a basis of the LION attack. When a PUEA is performed all SU have to release the band for employment by PU (spectrum mobility). When this spectrum handoff occur, the TCP running at Transport layer will be oblivious about this and will keep creating logical connections. Also the TCP at SU Transport layer continues to send packets to port number of the receiver without receiving any acknowledgments. When no acknowledgment is received TCP follows it's built in mechanisms like retransmission timer, fast retransmit etc. To make situation even worst, an attacker can create total network starvation, if he can anticipate the channel handed off and get hold of it by performing PUEA [47].

Summary

In this chapter the attacks relevant to Cognitive Radio were discussed with the layer they impact. The following chapter will give brief description of measures to counter these attacks.

Chapter 4

ATTACK MITIGATION STRATEGIES

4.1 Attack Mitigating Solutions

Security is the most critical aspect involved in the implementation of CRN, because if an attack (due to an unaddressed security issue) occurs, then CR will be unable to deliver its basic functionality that is the opportunistic access. To respond to this the need of developing secure protocols for the SU having mechanism such as authentication, authorization and encryption is a necessity. CRN is based on the premise that PU and SU are to be differentiated in the network, authenticating PU and SU is specifically mandatory since both PU and SU deserve different level of authorization and privileges to access the spectrum. Authentication can be easily implemented for centralized architectures by having a centralized authority; however it is difficult to implement such scheme in a distributed/ non-cooperative environment. The CRN provides conditional authorization. Conditional authorization refer to the term where the SU can only transmit in licensed frequency bands till the time the Primary User for that licensed band does not require that band. Encryption is a computationally difficult task to implement because of exhaustive key space and the overheads involved.

To respond to the diverse attack profile researchers have put in untiring efforts. Solutions to mitigate the attacks depicted in table 3.1 are discussed as follows.

4.1.1 Application layer

4.1.1.1 MW

In [41], to mitigate the possibility of a virus / MW; foremost, the authors suggest the relearning of radios to counter propagated false information through a feedback loop into the NW for consequent decisions. Furthermore, since principles are built in and certain principles are threshold principles violation of which will result in compromise. Hence, to invalidate learned actions by the CR that could possibly violate these principles authors suggest to build a logic into the CR.

4.1.2 Transport layer

4.1.2.1 KDA

In [31], the authors have suggested a method to delay key repetitions as key depletion occurs because of multiple sessions occuring at a fast pace due to excessive return trip phase and periodic recurrent transmissions. Key repetition delay by an exponential margin is suggested by employing a protocol for authentication of msgs/transmission incorporating a combination of CTR and CBC modes of encryption i.e. ctr block chaining employing a 48bit IV and using 128bit key.

4.1.3 Network layer

4.1.3.1 Sink-hole

Sinkhole attack is hardest to detect among other attacks in CRNs. However defence against this attack lies in development of protocols based on position-based routing. Position based routing build an on demand configuration employing only local transmissions and data without instigation from the BS. Using this scheme all the traffic is transmitted to the geographical location of the actual BS and it is hard to divert it to a MU for creation of a sinkhole [33].

Encryption and Link layer authentication are mechanisms on which techniques to mitigate sinkhole attack carried out by intruders external to the NW are founded. It may not be possible for outside attacker to join the NW when authentication is employed. Since, position-based routing would employ the mechanisms of encrypted transmissions and authentication to build an on demand configuration; hence, advertisement by the attacker as the efficient route would not be successful as members would only be employed by the CRN for routing [33].

Trust establishment updated recurrently is the mechanism on which techniques to mitigate sinkhole attack carried out by attacker internal to the NW is founded. This trust mechanism in CRN would employ central aggregation at BS/FC to which all issues and reports concerning deformed and dropped packets through a system will be forwarded. The data continuously being received at BS/FC would be analyzed and the NW members through a flood of messages will be cautioned about all the transmission problems encountered. Finally, the internal member of the NW found to breach the trust would be dropped from the NW.

4.1.3.2 Worm-hole

Wormhole attacks have sinkhole as an intrinsic part and it is hard to detect as well among other attacks in CRNs. However defence against this attack lies in development of protocols based on geographic / position-based routing for forwarding packets in the NW [33]. Position based routing build an on demand configuration employing only local transmissions and data without instigation from the BS physically towards the BS. Using this scheme all the traffic is transmitted to the geographical location of the actual BS and it is hard to divert it to a MU for creation of a wormhole/sinkhole. False link would be spotted by the local SU since it would observe the abnormal distance beyond normal radio range between themselves and the MU, or between the MU pair of wormhole and sinkhole.

4.1.3.3 HELLO

In [33], the authors proposed to employ symmetric key cryptography to counter Hello flood attack. Each node should share a symmetric key with trusted central authority. The two parties will share a symmetric key, which will provide two benefits; one is the authentication among the SU sharing the key and second is the SU will be able to encrypt the transmission. The number of shared keys should be limited so as to thwart an aggressor from initiating a session key with every SU whose the member of the NW. Moreover, generation of an alarm is proposed by the authors if numerous nodes in the NW find a single node declaring to be the neighbour of them all.

In [48], Authors propose a mechanism i.e. before link establishment verification of the bi-directionality of links through a message acquired over the very link can be used as a defence mechanism against the HELLO attack. BS/FC is employed as a trusted central (3^{rd}) authority for providing verification of bi-directionality and then onwards initiation of session keys to facilitate communication amongst SU of the NW.

Communicating SU /BS /FC verify each others identity through these session keys and secure their communication as well through an encrypted link. There should be a limit on the number of shared keys to prevent MU from establishing a link with every SU. It should be a warning sign if a SU(MU) is found to be a neighbor of mutiple number of SU even so which are located on mutli-hop distance.

4.1.3.4 Sybil

Authors in [35], discuss the presence of Sybil attacks in IEEE 802.11 networks and proposed a defence technique based on the statistics beacon transmission. The concept of signal prints based on multiple values of *"Received Signal Strength Indicator"* (RSSI) has been suggested in [36], to counter identity-based attacks in WSN, endorsement/ approval of every nodes identity is the essence of Sybil defense. Mechanisms to approve identities are classified into direct and indirect ways. In direct way, as is evident testing is to occur amongst two intercommunicating devices in which one being invoked for communication tests the validity of the other claiming to be some identity in the NW. In indirect way, approval for other devices is sought from earlier validated devices in the NW.

For direct approval in [49], means or asset test is presented as a technique. A supposition made with asset testing is that the means of the assailants (MU) physical device are exhaustible. To validate that every specified user is in possession of tested means as per its physical entity the testing of identities is carried out. Means accessible to Transmission/ communication, retention of data/storage and computation/ calculation are to be ascertained as suggested by the author. Foremost, the assumption that resources are limited and all nodes resource constraints are identical. Calculation could be tested by seeking concurrent solution to a peculiar problem from every device in the NW in a stipulated time. Storage could be tested by seeking retention of a huge proportion of

data that is not compressible by every device in the NW. To validate the confronted device/ identities have stored the information they are transmitted; the confronting device retains little portion of the information. Transmission could be tested by seeking replies to broadcast through which identities are sought from every device in the NW within a specified time limit.

An alternative approval/ verification technique is proposed by authors in [50] which may be appropriate in CRN. The testing technique put forth is based on radio resource, a supposition made with this testing is that each physical entity is in possession of a single radio. Furthermore, yet another supposition is that transmission and reception at any single moment in time by any radio is possible on a single channel. The validation process involves the allocation of separate unique broadcast channels to all devices in the neighbourhood by a challenging entity i.e. a device that wants to establish the absence/ presence of sybil identities in its neighbourhood. Challenger then listens on a randomly chosen channel from amongst the channels already allocated. If the transmitting device on the channel is the authorized entity which was allocated that particular channel in the initial process of channel distribution then the challenging device would be able to hear the transmission.

In [33], the authors proposed to employ symmetric key cryptography to counter sybil attack. Each node should share a unique symmetric key with trusted central authority i.e. BS/ FC. Initiation of session key amongst two intercommunicating devices in the CRN will be assisted by BS/ FC acting as a trusted 3rd pty. The two parties will share a symmetric key, which will provide two benefits; one is the authentication among the devices/SU sharing the key and second is the SU will be able to encrypt the transmission link amongst each other. The number of shared keys should be limited so as to thwart an assailant from initiating a session key with every device/ SU whose the member of the NW. Moreover, BS/ FC may enforce a restriction on the total permissible neighbours of a device. Consequently, generation of an alarm is proposed by the authors if numerous/ overabundant devices in the NW find a single node declaring to be

the neighbour of them all.

Finally [51, 52], most of the belief, reputation and trust techniques presented before or being presented after for other attacks can be implemented for sybil as well. Details of those methods could be sought from the other sections. Devices that breach trust intentionally or mistakenly, have been refuted by other entities and with low belief estimates will be penalized by being suspended, excluded or permanently dropped from the NW irrespective of being a sybil identity or a true unique entity.

4.1.4 Link layer

4.1.4.1 SSDF

The authors in [53] presented an analytical approach to counter SSDF attack. In the proposed scheme the performance bounds are indicated with respect to the proportion of SSDF attacks and attackers, which shades vision of the BS /FC.

In [54], the authors proposed a procedure which computes mistrustful degree of SUs built on their former behaviours. This procedure computes trust and consistency values (employed to remove the impact of MU on the PU sensing and identification results). For a node with fewer bad behaviours, the trust value recovers after a certain good behaviours, however the trust value is impossible to recover in case of regular bad behaviours.

In [55], the authors proposed a Bayesian detection scheme which entails knowledge of abstract conditional probabilities related to observation, discovery and identification results; in nutshell related to "sensing" results. Numerous cases/ instances occur based on the local and final sensing results, which can be either true or false. A low value is allocated to the true cases and a high value is allocated to the false cases. The all inclusive value is the total of all the values assigned previously weighted by the

probabilities of the comparable instances.

The authors in [56] proposed a weight based fusion scheme incorporating a trust approach and pre-filtering techniques. The process depends on information being pre filtered for identification and nullification of sometimes faulty and permanently faulty malicious users by assigning a trust factor to each user.

In [57], a fusion technique is proposed that collects sensing results from all nodes in the CRN. Then all the gathered results are summed. If the sum is greater than a certain threshold, then the final sensing result denotes that the PU is active else the channel is ascertained to be vacant, which means establishing absence of PU.

In [58], the Neyman-Pearson (N-P) test was proposed; it requires the user to define "maximum acceptable probabilities" of two things i.e. one is of false alarm and the second of miss. The N-P test pledges the defined probability to be acquired in contrast to other probability which is to be curtailed.

The authors in [59], proposed a detection scheme for SSDF attacks that works by keeping a tally of clashes amongst the local and global decisions at the BS /FC.

In [60], the authors proposed *"Weighted Sequential Ratio Test"* (WSRT) to confront SSDF attacks. In the proposed technique each node that has to perform sensing collects local sensing reports from neighbouring nodes. This scheme also employs belief estimate / reputation based mechanism. Each node is initially given a zero (0) equivalent belief estimate. Through every single true sensing account an increment of one (1) to the belief estimate will be made.

4.1.4.2 CCS

CCS can be mitigated by adapting a trusted architecture employing sequential probability ratio test. In the trust based architecture a dubious node will be observed, examined,

assessed and judged by its neighbours. Based on monitoring the neighbour can then perform a sequential analysis on observed data, and determine whether a node is acting maliciously or not [61].

In [54], the author introduces a technique to respond to CCS with an substitute rendezvous (RV) negotiation based decision making strategy to ensure coordination of communication amongst SU. Authors present a mathematical evaluation of the means essential for channel arbitration in the NW built on the count of SU available and the present channel throughput. When the CCC utilization nears the extremity at which further allocation of means to RV channel arbitration will generate a inundated situation, the NW proceeds to the point of RV channel arbitration. This technique evades the condition through which CCS is attained and there are no means left for further channel RV arbitration. Consequently, preliminary channel evaluation and inception of arbitration averts the depletion of data channeling means while the CCC is overwhelmed.

4.1.4.3 CCC

In [62], the authors present methods to mitigate CCC for Distributed/ "ad hoc" NW built around clusters employing hopping sequences. The NW is divided into little groups managed by a cluster head which determines the operating CC and hopping sequences for the cluster. Owing to the characteristics of clustering in the NW when jamming attacks a cluster, the influenced NW zone is a small fraction.

4.1.5 Physical layer

4.1.5.1 Jamm-ing

Since DoS attack by Jamming can affect both Link layer and Physical layer. At Link layer detecting DoS can be by sensing the channel the SU want to use for their transmission. Employing carrier-sensing multiple-access (CSMA) may provide the desired result. In CSMA, node continually senses a channel until it finds it to be idle and upon finding a channel as idle the node waits a prearranged span prior to initiation of transmission ("propagation delay") to guarantee or ensure channel is vacant.

At Physical layer the legitimate SU would be capable to differentiate amongst the usual and unusual extent of disturbance in a channel i.e. Signal to Noise (SNR) ratio. This can be done by collecting data regarding the SNR in the CRN and then constructing a statistical model to employ for comparison when a DoS occurs [40].

In [63], the authors suggested Signal Strength Consistency Checks, a jamming detection technique that inspects the *"Packet Delivery Ratio"* (PDR) and *"Signal Strength"* (SS). PDR is the ratio of packets delivered to packets sent. If SS is high and PDR is low it is assumed that jamming of the channel is being carried out, except if any of the neighbours has both PDR and SS as high. Another procedure named Location Consistency Checks is suggested, where the place of the neighbours is important. Location information is advertised by each node and can be acquired through GPS. A node is considered as jammed when its neighbours have low PDR.

In [48, 64], authors have suggested detection of Jamming through triangulation and energy based techniques. Time is of the essence in such scenarios and the time lost with the suggested techniques would allow the attacker to severely impact the network. Furthermore, difficulty to locate mobile attacker further complicates the situation.

4.1.5.2 OFA

In [65], threshold values are defined by the authors for each and every adaptable radio parameter. Threshold values are the red lines / limits, if the SU radio parameters do not satisfy the limits, the communication stops. IDS based solution is also suggested by the authors. The straight forward definition of thresholds for each of the adaptable parameters would make it easy for a MU to guess the thresholds of other SU. Communication would be prevented if the predefined threshold is not fulfilled by one or more of the parameters.

In [66], the author uses a methodology of adaptable localized detection threshold for each SU that adapts on the state differences diminishing behavior, taking benefit of the property of state convergence. For an MU to guess at any instance all the threshold values of other SU becomes inadvertently more difficult under this methodology. MU beneath the straight influence/direct collaboration of an infected SU/ other SU of the attacked NW might not be a possibility to halt; OFA can be especially hard to prevent in such a scenario.

4.1.5.3 PUEA

Almost all types of selfish and few less than all malicious attacks are intrinsically PUEA and the mitigation techniques applicable to the bulk of them are applicable to PUEA mitigation as well. Never the less, In [67], the author presents a localization method formed on transmitter RSSI. Correction technique triangulation taking into account refraction and multipath signals gives a refined localization method. In CRN each SU carries out spectrum sensing from time to time and communicates the measurement outcome to the BS/ FC. BS/ FC aggregates this data and analyzes the presence of PU. BS/ FC may be mislead and determine the PU is transmitting if a MU injects false positive offset data.

4.1.5.4 OSU

The use of direct sequence spread spectrum (DSSS) and frequency hopping (FH) can make effective DoS difficult to launch. DoS may still degrade QoS. Moreover, observing PU signal characteristics and location can be helpful for identification of a MU by the NW.

In [54], the authors present a scheme which is modeled to ascertain a consistency value, belief value and suspicion level for identification and sidelining of a MU. SU become suspicious when there is disparity between reported channel state by a MU and the channel state reported by other SU. This is a consensus scheme, trust value and consistency value reflecting the level of trust and consistency of trust respectively is calculated over time for each SU. SU with a regular less belief value will consequently be distinguished as a potential MU and excluded from the NW.

4.1.6 Cross layer

4.1.6.1 RIJ

In [68], authors present a solution in which a SU selects a resident channel. This selection is then broadcast to its neighbors. Any updates of the CR are expected to be received by SU on this resident channel. The issue with this solution is that it puts an overhead on normal radio communication which is half duplex with single channel occupancy. This solution necessitates presence of two half duplex transceivers on every SU i.e. for data transmission channel and one for resident channel so that control message exchange takes place on it.

4.1.6.2 SBW

In [69], authors proposed that between successful transmissions idle slots could be a cause of SBW. Hence, the number of idle slots be measured.

In [45], propose a trust-based cross-layer defence framework that take the coordinated approach of these two attacks SBW(MAC layer) and SSDF(PHY layer) and plays its part to defend against these. The authors present a strategy in which the corresponding receiver provisions the backoff window span and monitoring of a sender. Any deviation from assigned values results in punishment i.e. larger value for further communication, on continuity of violations the node will be ejected from the NW.

This strategy mentioned above fails if receiver and sender collude with each other or if the receiver for its own transmissions purposely assigns large backoff values. This can be addressed by observation of the backoff by multiple number of SU . Furthermore, it can be addressed if a PRNG is used to produce the backoff window estimate which is known publicly or every CR broadcasts its backoff plan beforehand [70].

4.1.6.3 JFA

The JFA is a passive attack as it follows all protocol rules. In [71], author proposed a novel solution jellyfish attacks mitigator (JAM).

In [71], authors suggest using the broadcast capability of the wireless medium for countering JFA. JFA can be detected by neighbouring SU set as promiscuous simultaneously. On experiencing low throughput in the NW, catalyst helper packets are transmitted by adjusting TCP protocol which are supplied with a flow id number and cumulative sequence numbers to check for congestion. Since, this is a collaborative scheme any discrepancy is observed by all SU and any misbehaving SU is punished by ejecting out of the NW plus it may also lead to revocation of certificate by some

monitoring CA.

In [72], present an idea for pure ad hoc CRN i.e establishing and managing trust of a network through a trust based mechanism. Muti-hop routing protocols are modified to give threshold values to SU and based on that to routes as well. SU first checks these threshold values before transmission to another SU. Consequently, based on threshold estimate insufficiency path will be avoided.

In [73], authors present a robust and scalable collaborative approach for a dynamic mobile ad hoc CRN architecture. each SU observes its neighbourhood. A threshold for packet drop is defined, if any neighbour SU drops packet at a rate greater than the defined threshold which is based on a specific time rate then misbehaving SU is punished by ejecting out of the NW and is isolated for a time period.

4.1.6.4 LION

In [47], authors suggested employing data sharing among physical, link and transport layers. To achieve confidentiality and authentication in CRN Group Key Management (GKM) was proposed. Since, LION attack is a cross-layer attack by enabling the cross layer communication the TCP protocol is made aware of what is happening at the physical & link layer.

In [74], author suggests to use a cross-layer IDS to find the attack source alongwith cross-layer communication for the purpose of assuring TCP is conscious of the intruder/ attack. TCP awareness leads to CRN halting TCP connections during handoffs. Moreover, to secure the common control channel from the eavesdropping a GKM can be used. In [74], the authors suggest usage of a shared secret. Shared key provision will allow neighbourhood SU to authenticate, encrypt and decrypt control data. The key would need to be updated as the members move in and out. Hence, GKM be utilized in CRN as a solution.

In [75], author suggest a TCP variant called Freeze-TCP in mobile ad-hoc CRN architecture where disconnections are frequent to improve the performance of TCP.

Cross layer transmission and GKM can only attenuate this attack; QoS degradation or DoS due to jamming can't be stopped.

Summary

In this chapter the countermeasures relevant to attacks in Cognitive Radio were discussed based on the mitigation strategy they employ. The following chapter will give an analysis to the discussions till now.

Chapter 5

ANALYSIS

5.1 Introduction

CRN is characterized by its heterogenous nature and interconnectivity where smart SDR interact with each other for data. Focal attraction of CRN is its real-time opportunistic operation to sense, process, adapt and act to perform prescribed operation autonomously. Based on these features CRN has its application and utility in almost all wireless technologies. Its cost effectiveness, interoperability, seamless connectivity, scalability, autonomous operation and extensibility are collectively the notion based on which CRN is gaining interest all around the world and has towering future prospects in terms of adoption. But this huge scale adoption is linked to security challenges. Large scale implementations will also increase attack surface for adversaries compared to present day NWs thus creating immense challenges to address security concerns. Traditional security solutions, methodologies, techniques and procedure involves implementation of security mechanisms such as IDS, IPS, AV, VPN, IP Sec, SSL/TLS, encryption algorithm, signal fingerprinting and many others. In this context, the key question is "can these security solutions be employed in CRN architecture for security". To answer, considerations pertaining to constrained resources in CRN such as bandwidth capacity, sensing, processing, adaptation and action (power output) must be

examined and analyzed. Likewise, key elements such as wireless connectivity and CR mobility introduces added security requirements for CRN ecosystem.

5.2 Issues in CR - CRN

5.2.1 Identity Management (IM)

Among many security challenges to CRN, identity management (IM) is a crucial element in CRN protection. IM ensures the correct control of CRN entities; where it contributes towards authentication and authorization of a CR. IM is linked to security since it enables a CR in a CRN to correctly access and collaborate among themselves and with BS/FC.

5.2.2 Authentication

Without authentication mechanism, there will be no way to ascertain that received data is from legitimate CR and the content it contains is not altered during transmission. IM plays a vital role for authentication process as various CR needs to authenticate each other for trusted communication.

5.2.3 Authorization

Authorization is a process of allowing requisite access to authenticated entity. In CRN domain PU and SU are distinct entities therefore merits distinct rights which creates complexities for access mechanism. Without proper authorization, adversary can introduce rouge device (MU) for malicious activity.

5.2.4 Encryption

Main classification of data encryption are asymmetric and symmetric. Both the encryption methodologies have their own advantages and disadvantages for computing systems. In CRN perspective where CR are involved for their prescribed functionality have limitation vis-à-vis computational ability, storage, energy availability and bandwidth capacity; therefore, asymmetric encryption algorithm complexity and its requirement for resources makes it difficult to implement in such environments. On the other hand, implementation of symmetric encryption is suitable for CRN domain due to simple and small amount of calculations.

5.2.5 Jamming

As CR have to employ processing, memory, power and bandwidth capacity opportunistically and efficiently therefore jamming attack is far more effective against them. Since, CR communicate utilizing wireless white spaces therefore the prime methodology for attacker is to carry out jamming attack. Alternatively, wireless communication media can experience interference from other co-located devices thus can create unintentional jamming. In any case, device will not be able to communicate among each other thus a major challenge in CRN domain.

5.2.6 Availability

It is crucial that CR should remain available for intended functions. The CR functionality can be effected due to malfunctions or malicious activity and may no longer remain available to legitimate user. Similarly, availability issues can be created due to battery drainage, theft or damage to device. In this context, security and requisite mechanisms at all layers starting from physical to application layer can address availability concerns. Careful study and planning is required to employ security solutions and administrative

mechanism according to available resources.

5.2.7 Deployment Architecture

The concept of CRN can be summarized as "opportunistic access of frequency spectrum". Diverse approaches can be utilized in order to implement the vision of CRN for exploitation of vacant spaces in frequency spectrum. Primarily, Centralized and Distributed architecture can be implemented to deploy CR in a CRN and a combination of both. Centralized architecture, which is basically client-server architecture where there is a central entity i.e. BS/FC with which CR are connected and there is not much support to directly access CR. The CR in Centralized architecture can exchange intelligence with other CRN and creates new enriched services. Alternatively, in a Distributed or decentralized architecture various CR in a CRN collaborate with each other dynamically. Both the architectures have different feature and advantages which are analyzed in succeeding sections.

5.2.7.1 Centralized CRN Security Management

CRN is collection of smart SDR a.k.a CR in a NW which interact with each other. In this context, security is amongst the critical issues which needs to be addressed for the success of CRN. It is therefore imperative that interactions must be protected along with restricting the incidents which can cause harm to CRN. The amount of attack vectors available to adversaries is also growing as compared to present day connectivity. In this section analysis of security concerns has been carried out to assess the effectiveness of Centralized architecture.

5.2.7.1.1 Identity and Authentication (IAM) : The foremost element is to identify and authenticate an entity into a NW without which desired services cannot be made available or the adversary can incorporate himself as trusted entity. In Centralized ar-

chitecture, this issue is simple to handle due to presence of single central entity known as BS/FC with which other CR are connected. Specifically, effective IAM can be installed in a BS/FC to offer better control and to create limited set of entry points into the NW. Each time a new CR attempt to access the NW, it has to authenticate itself to BS/FC before accessing the NW.

5.2.7.1.2 Access Control - Authorization : Like IAM, the access control mechanism is also simple to implement due to BS/FC. Access control rights can be configured in BS/FC from where access to legitimate CR is granted to access required resources. As access right are configured in single BS/FC therefore simplicity and better control is involved in implementation and management.

5.2.7.1.3 NW Security : Security challenges such as negotiating of security algorithms and selection of protocols requires deliberation in implementation in constrained environment. Criticality of data, amount of data, accessibility to NW, integrity requirement and number of security protocols must be considered for implementation of security mechanism.

In case of Centralized architecture, the BS/FC is efficient in terms of bandwidth utility, computational resource, storage and power output to implement security mechanisms. Moreover, upgrading and patching of NW security mechanism is also manageable due to availability of resources in BS/FC.

5.2.7.1.4 Device Security : CR in CRN has to perform its prescribed functionality which includes, sensing and collection of spectrum data, processing, interacting with other entities, data storage and performing stipulated operation. All this functionality requires well managed processing, power, memory and bandwidth. Adversary will attempt to manipulate the CR operation or corrupt it to not perform its prescribed functionality. CR security requires processing and memory to carryout security operation.

Addition of security mechanism to normal operation can create extra load on processing and memory. In this context, HW and SW specification merits careful deliberation and analysis to balance out both normal operation and security requirement.
In Centralized architecture, heavy processing and large data storage are delegated to single central unit which conserve processing and memory in CR for security mechanism. This leverage is one of the prime trademark of Centralized architecture where security mechanism can be hosted without affecting normal operation of CR in a NW.

5.2.7.1.5 Data Security : Security of data either stored or in transit is one of the prime security concern. In CRN security of data can be achieved by using cryptographic algorithm. In this regard, a significant decision is involved whether to use symmetric encryption or asymmetric encryption. Secondly, key management is another factor which needs optimal handling in establishing data security. Encryption itself consumes high processing resources especially asymmetric encryption. Light weight encryption algorithms are the solution which consume less processing power. In Centralized architecture, the central entity i.e. BS/FC has sufficient processing capability and memory to employ required encryption mechanism. So, asymmetric encryption can be used for external communication services. On the other hand, symmetric encryption which consume less resources can be used between central entity i.e. BS/FC and CR. However, symmetric encryption requires effective key management because loss of key can compromise the entire security.

5.2.7.2 Distributed CRN Security Management

In Distributed deployment of CRN, the CR interact with each other and due to dynamic nature of Distributed architecture, each CR needs to be secured separately. Security implementation on each CR requires careful evaluation of constraints of each CR such as processing, power and memory. The adversary can control part of the CRN or few CR but due to distributed nature of NW, it is difficult to bring down the entire CRN.

There are wide range of security challenges to Distributed CRN, analysis of few are as under: -

5.2.7.2.1 Identity and Authentication (IAM) : This feature is bit complex in Distributed architecture as compared to Centralized architecture of CRN. In Distributed architecture, CR interact with each other directly. Therefore, IAM needs to be implemented on every CR and requires deliberate efforts to generate trust within the CRN.

5.2.7.2.2 Access Control - Authorization : In Distributed CRN deployment, the challenges of access control are same as of IAM. Wide variety of CR in distributed CRN would be operating autonomously therefore creating complications in access control policies. Each CR or group of CR in Distributed architecture needs to be configured separately for access policies. This separate configuration of CR also creates management problems which needs effective management schemes to achieve efficiency.

5.2.7.2.3 NW Security : Selection of security parameters, algorithms and protection mechanisms necessitate evaluation, as each of the procedure has its own processing overhead including power and memory. In distributed architecture, each CR in a CRN needs to be configured separately according to task and functionality of the CR.

5.2.7.2.4 Device Security : In Distributed CRN, security of CR itself is important. Securing each CR needs careful planning and monitoring, any bug or vulnerability left can compromise the CR. Moreover, security audit of Distributed architecture is also complex in terms of time and large number of CR in a CRN. Securing each CR is challenging due to non-availability of single interface for number of CR and also creates complexity in their security audit. In Distributed architecture for CRN, tradeoff will always remain between normal functionality and security mechanism.

5.2.7.2.5 Data Security : Processing overhead of asymmetric encryption is more compared to symmetric encryption. As symmetric encryption requires less processing overhead therefore preferred scheme for Distributed CRN. In symmetric encryption, key management has a pivotal role for security of data. In symmetric encryption, if key is compromised then entire data security mechanism is lost. In Distributed architecture, key establishment is very challenging due to large number of CR and non-availability of single interface to interact with each of the CR.

5.2.7.3 Architecture Analysis

The discussion and analysis of CRN Architecture can be summarized as depicted in the Table 5.1:

Table 5.1: Architecture Analysis

Attributes	Centralized	Distributed
Security Mangement	Security in CRN through BS/FC	Each CR is required to be configured individually
Identity and Authentication	CR to BS/FC, Easier to implement	collaborative CR to CR, Challenging
Access Control	Managed through BS/FC, Simple to implement	Requires detailed management through collaboration
NW Security	Governed through BS/FC, Better control and management	complex, requires detail analysis

Attributes	Centralized	Distributed
Device Security	Processing and transmission of collected data through BS/FC, Conserving resources in device for security	Additional local resources required for security mechanism and balance needed between security and normal functions
Data Security	Effective encryption-key management	Deliberation required for key management

5.3 Attacks and Countermeasures

In the following subsections attacks and their countermeasures summary is depicted in tabular form .

5.3.1 Attack Analysis

The summary of attacks vis-à-vis layers, the attack vector involved, the source of the attack are listed in Table 5.3.

Table 5.3: Attack Analysis

Layer	Attack	Description	Source	Objective (Malicious /Selfish)	Impact (Induced /Direct)	Domain (Conventional /CRN)	Architecture Impacted Most	Scope (AIC)	Detail
Application	MW	Tampering of software of SDR	Both	Malicious	Both	Conventional	Distributed	A	[32] [30]

continued overleaf

Table 5.3 : Attack Analysis

Layer	Attack	Description	Source	Objective (Malicious /Selfish)	Impact (Induced /Direct)	Domain (Conventional /CRN)	Architecture Impacted Most	Scope (AIC)	Detail
Transport	KDA	Repetition of the same key twice due to the large number transport layer sessions in CRN	Internal	Malicious	Induced	Conventional	Distributed	IC	[30]
Network	Sinkhole	Assailant publicizes itself as the shortest path and tries to attract nodes to move their traffic	Internal	Mailicious	Direct	Conventional	Mesh Infrastructure	AIC	[34]
	Wormhole	Attacker tunnel packet it receives at one end of the NW through a low-latency channel and then start replaying in other portion of the NW	Internal	Malicious	Direct	Conventional	Mesh Infrastructure	AIC	[33]
	HELLO	Attacker broadcast HELLO packets to convince other node that it is their neighbour	Internal	Malicious	Direct	Conventional	All	A	[33]
	Sybil	A single node uses multiple fake identities and pretends to be present at different location of the network at once	Internal	Both	Direct	Conventional	Distributed	A	[35] [36]

continued overleaf

Table 5.3 : Attack Analysis

Layer	Attack	Description	Source	Objective (Malicious /Selfish)	Impact (Induced /Direct)	Domain (Conventional /CRN)	Architecture Impacted Most	Scope (AIC)	Detail
MAC	SSDF	Attackers transmit fake local spectrum sensing observations to the FC/neighbours	Internal	Both	Direct	CRN	Distributed	A	[10] [33] [31]
	CCS	CR decides to defer transmission in subsequent data phase if in control phase restricted time it can not broker due to saturation of CC	Internal	Both	Induced	CRN	Distributed	A	[37]
	CCC	Jamming of the CC to disrupt the communication and collaboration in the network	Both	Malicious	Direct	CRN	Distributed	A	[38]
Physical	Jamming	It disrupts the communication by high power signal or malicious packets or making interference (SNR) with the radio signal	External	Malicious	Direct	Conventional	All	A	[39] [40]

continued overleaf

Table 5.3 : Attack Analysis

Layer	Attack	Description	Source	Objective (Malicious /Selfish)	Impact (Induced /Direct)	Domain (Conventional /CRN)	Architecture Impacted Most	Scope (AIC)	Detail
Physical	OFA	Misleading and manipulating the cognitive core of the cognitive engine of the CRs for not employing the optimum transmission parameter	Internal	Both	Induced	CRN	Distributed	A	[41]
	PUEA	A malicious user masquerade as a primary user to obtain the exclusive access of a given channel	Both	Both	Direct	CRN	Distributed	A	[13] [14]
	OSU	A CR on the perimeter of overlapping co-existent CRN may initiate transmissions that may impair the PU and SU through an error or malicious intent	Both	Malicious	Direct	CRN	All	A	[42] [37]
Cross	CAA	MU affects the learning algorithms by transmitting misleading channel assignment (CA) information to other SU which leads to generation of series of changes in CA in the multi-hop environment	Internal	Selfish	Induced	CRN	Distributed	A	[44]

continued overleaf

Table 5.3 : Attack Analysis

Layer	Attack	Description	Source	Objective (Malicious /Selfish)	Impact (Induced /Direct)	Domain (Conventional /CRN)	Architecture Impacted Most	Scope (AIC)	Detail
Cross	RIJ	A assailed CR is forced to commence handoff prior to exchange of information on routing	Internal	Both	Direct	CRN	Distributed	A	[31]
	SBW	A malicious user selfishly decreases the back off window size to gain priority on channel access	Internal	Selfish	Induced	Conventional	All	A	[45]
	JFA	Attacker intentionally delays or mis-order the data packets it receives and transmits	Internal	Malicious	Induced	Conventional	Distributed	A	[31] [45] [46]
	LION	Uses the PUE attack to disrupt transmission control protocol (TCP) connection	Both	Both	Direct	CRN	Distributed	A	[47]

5.3.2 Countermeasure Analysis

The summary of attack countermeasures vis-à-vis mitigation technique, strategy, trust based or not, the overhead involved in implementation, the contribution and suggested consideration for refinement of solution are listed in Table 5.4.

Table 5.4: Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Application	MW	Relearning of radios/CR	To invalidate learned actions by the CR that could possibly violate these principles a logic to be built into the cognitive core.	No	High	Simple rollback of complete learned logic from the time of start of transmission/reception. A chronological log sequence for establishing inception of attack for segregating attacking node would pay dividends if incorporated.	[41]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Transport	KDA	Delay key repetitions	Key repetition delay by an exponential margin is suggested by employing a protocol for authentication of msgs/transmission incorporating a combination of CTR and CBC modes of encryption i.e. ctr block chaining employing a 48bit IV and using 128bit key.	No	High	Thorough cryptanalysis of the proposed solution needs to be carried out to establish any weakness in the implementation mechanism of the proposed combination of the cipher mechanism.	[31]
Network	Sinkhole	Secure Protocol based on position-based routing	External : Encryption and Link layer authentication are mechanisms on which techniques to mitigate sinkhole attack carried out by intruders external to the NW are founded. Internal : Trust establishment updated recurrently is the mechanism on which techniques to mitigate sinkhole attack carried out by attacker internal to the NW is founded.	External : No Internal : Yes	External : High Internal : Average	PU activity and spectrum availability not taken into consideration through the process involving forwarding of data.	[33]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Network	Wormhole	Protocol based on position-based routing	Pre-phased route-topology to BS/FC would be chalked out and any new advertised route will be bypassed.	No	Average	Challenging in distributed architecture. Trust mechanism needs to be incorporated for addressing rogue nodes and expelling them.	[33]
	HELLO	Node identification	Symmetric key cryptography for two fold objective; foremost, authentication then encryption of transmission. Furthermore, eneration of an alarm in the NW on detection of node to be neighbor of multiple entities.	No	High	Additional HW for encryption a necessity. Procedure of stern action against rogue node needs to be incorporated.	[33]
		verification of the bi-directionality of links	BS/FC is employed as a trusted central (3^{rd}) authority for providing verification of bi-directionality and then onwards initiation of session keys to facilitate authentication and encrypted communication amongst SU of the NW.	No	High	Challenging in distributed architecture. Trust mechanism needs to be incorporated for addressing rogue nodes and expelling them.	[48]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
		Statistics beacon transmission	Sybil entity beacon transmission anomalies are assessed. At the receiver end beacon interval statistics are assessed to segregate amongst legitimate and sybil node transmitted beacon frames.	No	Average	Mechanism for filtering of false positive and negatives needs to be streamlined as is a necessity in analytical methods.	[35]
Network	Sybil	Signal prints based on Indicator of Received Signal Strength (RSSI)	A transmiter can be uniquely identified on base of signalprints; which based on a location are unique.	No	Avergae	Longer distances result in false positives due to reduction in sensitivity. Combining with geographical routing will produce refined results.	[36]
		Resource Testing model	communication, storage and computation testing for validation of identities in a NW through a coordinated simultaneous effort by all nodes.	Yes	High	A hypothetical Abstract model involving stringent assumptions as in simultaneous validation involving broadcast, extensive computation and storage usage less practical in implemented heterogeneous NW having nodes with varying resources.	[49]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Network	Sybil	Testing radio resource	Involves the allocation of separate unique broadcast channels to all devices in the neighbourhood by a challenging entity and then listening to transmissions to see that the entity is the one which was assigned the channel.	No	High	Suppositions are that each physical entity is in possession of a single radio and transmission/reception at any single moment in time by any radio is possible on a single channel which may not be true in case of an over resourced assailant in posession of customized HW.	[50]
		Node identification	Symmetric key cryptography for two fold objective; foremost, authentication then encryption of transmission. Furthermore, eneration of an alarm in the NW on detection of node to be neighbor of multiple entities.	No	High	Challenging in dynamic distributed architecture.	[33]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Network	Sybil	Belief, reputation and trust techniques	Devices that breach trust intentionally or mistakenly, have been refuted by other entities and with low belief estimates will be penalized by being suspended, excluded or permanently dropped from the NW	Yes	High	A true unique entity in danger of being penalized as well.	[51]
MAC	SSDF	Analytical approach	Performance bounds are indicated with respect to the proportion of SSDF attacks and attackers, which shades vision of the BS /FC.	Yes	Average	Involves BS /FC, valid for centralized architecture not distributed.	[53]
		Identification process on belief value	Computes suspicion degree of SUs employing trust and consistency values built on their former behaviours.	Yes	Average	Adressing of numerous MU simultaneously an issue.	[54]
		Bayesian detection scheme	Entails knowledge of abstract conditional probabilities related to observation, discovery and identification results i.e. a priori information.	Yes	Average	Analytical approach based on a priori information which can be corrupted by ssdf attack.	[55]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
		Weight based fusion scheme	Process depends on information being pre filtered for identification and nullification of sometimes faulty and permanently faulty MU by assigning a trust factor to each user.	Yes	Average	Severe attack impact resulting in performance degradation unaccounted for.	[56]
		Fusion technique	Collects sensing results from all nodes in the CRN which are then summed and compared to a threshold value for finality of decision.	No	Average	Threshold as a fixed benchmark causes false positive/negatives which aggravates further under severe attack.	[57]
MAC	SSDF	Neyman-Pearson (N-P) test	False positive or False negative acceptability probability limit has to be defined by the user.	Yes	High	Analytical approach based on a priori information which can be corrupted by ssdf attack.	[58]
		Identification scheme at the BS /FC	works by keeping a tally of clashes amongst the local and global decisions at the BS /FC.	Yes	Average	Works only in centralized architecture and foregos distributed architecture.	[59]
		WSRT	Employs maintenance of reputation followed by a hypothesis test	Yes	High	Processing overhead at each node as it carries out the process locally.	[60]
	CCS	Trusted architecture employing sequential probability ratio test	Dubious node will be observed, examined, assessed and judged by its neighbours who will then perform a sequential analysis on observed data, and determine whether a node is acting maliciously or not.	Yes	High	Legitimate node stands the danger of being penalized as well by an erroneous move.	[61]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
MAC	CCS	Substitute rendezvous (RV) negotiation	Mathematical evaluation of the requirements essential for channel arbitration in the NW built on the count of SU available and the present channel throughput.	No	Average	This technique evades the condition through which CCS is attained; rogue nodes are not earmarked.	[54]
	CCC	Clustering	The NW is divided into little groups managed by a cluster head which determines the operating CC and hopping sequences for the cluster. Owing to the characteristics of clustering in the NW when jamming attacks a cluster, the influenced NW zone is a small fraction.	No	Average	Detection of MU not accorded for it bypasses the jammed channels.	[62]
Physical	Jamming	Statistical model based on SNR	Collecting data regarding the SNR in the CRN and then constructing a statistical model to employ for comparison when a DoS occurs	No	Average	When would the data be enough for building the model.	[40]
		Location consistency check	Location information is advertised by each node and can be acquired through GPS. A node is considered as jammed when its neighbours have low PDR.	No	High	GPS presence becomes essential with each node which is not always the case.	[63]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Physical	Jamming	PDR Vs SS	PDR is the ratio of packets delivered to packets sent. If SS is high and PDR is low it is assumed that jamming of the channel is being carried out, except if any of the neighbours has both PDR and SS as high.	No	Average	Way forward on marginal difference not accorded for; no benchmark set for low or high.	[63]
		Triangulation	Detection through triangulation and energy based techniques. Good for detecting static attackers.	No	Average	Time lost would allow the attacker to severely impact the network. Difficulty to locate mobile attacker further complicates the situation.	[64]
	OFA	IDS	Detection of any abnormal behavior	No	Average	A general approach with no stopping measure whatsoever.	[65]
		Adaptable localized detection threshold	Methodology of adaptable localized detection threshold for each SU that adapts on the state differences diminishing behavior, taking benefit of the property of state convergence.	No	Average	Collusions cannot be ruled out.	[66]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Physical	OFA	Threshold values	Threshold values to be defined for each and every adaptable radio parameter. Communication would be prevented if the predefined threshold is not fulfilled by one or more of the parameters.	No	Average	The fix straight forward definition of thresholds for each of the adaptable parameters would make it easy for a MU to guess the thresholds of other SU.	[65]
	PUEA	Transmitter RSSI	A transmiter can be uniquely identified on base of signalprints; which based on a location are unique. Correction technique triangulation taking into account refraction and multipath signals gives a refined localization method.	No	Average	Injection of false positive offset data by MU cannot be ruled out.	[67]
	OSU	Identification process on belief value	Computes suspicion degree of SUs employing trust and consistency values built on behaviours.	Yes	Average	Adressing of multi MU simultaneously an issue.	[54]
Cross	RIJ	Selection of resident channel	SU selects a resident channel which is then broadcast to its neighbors. This solution necessitates presence of two half duplex transceivers on every SU i.e. for data transmission channel and one for resident channel so that control message exchange takes place on it.	No	High	The issue with this solution is that it puts an overhead on normal radio communication which is half duplex with single channel occupancy.	[68]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
		Idle slots measurement	Between successful transmissions idle slots could be a cause of SBW. Hence, the number of idle slots be measured.	No	Average	Idle slot measurements without earmarking rogue nodes would bypass the cause.	[69]
Cross	SBW	Trust-based cross-layer defence framework	Corresponding receiver provisions the backoff window span and does monitoring of a sender. Any deviation from assigned values results in punishment i.e. larger value for further communication, on continuity of violations the node will be ejected from the NW.	Yes	High	Strategy fails if receiver and sender collude with each other or if the receiver for its own transmissions purposely assigns large backoff values.	[45]
		Public watch and PRNG	Receiver and sender collusion can be addressed by observation of the backoff by multiple number of SU. Furthermore, a PRNG is used to produce the backoff window estimate which is known publicly additionally every CR broadcasts its backoff plan beforehand	No	High	Involves a lot of overhead in public watch and computation.	[70]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
		Jellyfish Attacks Mitigator - (JAM)	On experiencing low throughput in the NW, catalyst helper packets are transmitted by adjusting TCP protocol which are supplied with a flow id number and cumulative sequence numbers to check for congestion. A collaborative scheme where misbehaving entity is punished by ejecting out of the NW.	Yes	Average	Colluding nodes need to be addressed and isolated.	[71]
Cross	JFA	Trust based mechanism for route trustworthiness	Muti-hop routing protocols are modified to give threshold values to SU and based on that to routes as well. SU first checks these threshold values before transmission to another SU.	Yes	Average	Time elapsed trust value and collusion of nodes for malicious behaviour needs to be addressed.	[72]
		Robust and scalable collaborative approach	A threshold for packet drop is defined, if any neighbour SU drops packet at a rate greater than the defined threshold which is based on a specific time rate then misbehaving SU is punished.	Yes	Average	Enforcement of collaboration can be exploited for collusion.	[73]

continued overleaf

Table 5.4 : Attack Countermeasures Analysis

Layer	Attack	Countering Technique	Strategy	Belief Mechanism (Yes/No)	Overhead (High /Average)	Assessment	Reference Work
Cross	LION	Cross layer detection and mitigation	Employing data sharing among physical, link and transport layers for TCP optimization; secondly, to achieve confidentiality and authentication for control data employment of Group Key Management (GKM) and finally IDS utility. All of these are to be employed in tandem.	No	High	Overhead quite high due to simultaneous application of multi faceted security framework. QoS degradation or DoS due to jamming can't be stopped.	[74]
		Freeze-TCP	A TCP pro-active variant employed in an environment where disconnections are frequent to improve the performance of TCP incorporating prediction by receiver of possible disconnections.	No	Average	when entering a new, unknown environment full rate restart of transmission with the old window size starts before congestion state sampling. The need to be pro-active demands the receiver to predict impending disconnections.	[75]

5.4 Security Model

The highlight of the discussion so far specifically the analysis is that Cognitive Radios are constrained by their specific purpose of cognitive functionality i.e. the working of their cognitive core / engine. Cognitive Radio being an intelligent and smart SDR that adapts opportunistically to its environment based on dynamic variables has seemingly a difficult task at hand to have security solutions whether locally or globally implemented in its eco system as compared to traditional wireless networks that have matured over-time.

Traditional wireless NWs are hard programmed with policies and the only overhead they encounter are these coupled with the security solutions enforced in their environment. On the other hand Cognitive Radios in a CRN not only adhere to inbuilt policies but have a cognitive engine which is in a continuous learning phase which grows and expands its logical DB with passage of time; now the overhead of these two processes along with the security solutions that would be placed in the CRN ecosystem locally on the Cognitive Radios and globally at the Base Station (BS) / Fusion Centre (FC) would impinge the normal functionality of the Cognitive Radios. Nevertheless, security cannot be foregone but the point to ponder is that CR / CRN not only face the onslaught of the attacks prevalent in the conventional/ traditional wireless NWs but attacks that are pertinent and peculiar only to the CR domain.

The solutions and strategies to address attacks in the conventional/ traditional wireless NW domain have matured over time and are part & parcel of the TCP/ IP stack protocol implementations which can also effectively and efficiently address the same in the CR / CRN ecosystem being TCP/ IP based itself. However, solutions and strategies for attacks peculiar to the CR/ CRN domain are mere proposals and have yet to see the light of the day. The reasons of non-maturity of solutions is that CR/ CRN are still evolving; they are in the developmental phase with no standardization as such except for the draft version of IEEE 802.22 standard specific to use of Cognitive Radios

for provision of broadband services to thin density geographical area i.e. rural entities on long range employing TV broadcast band whitespaces. Another reason is there is no current deployed practical application of CR/ CRN which eventually restricts the test bed for these solutions and strategies which address attacks peculiar to the CR/ CRN domain. The projected recommended deployment may not be possible even until 2020 then only the maturity of these solutions and strategies can be stress tested in real, dynamic running environments. These issues should not be a hindrance for evolution of security solutions because the development, refinement and enhancement have to go hand in gloves before the actual deployment.

Having presented diverse stand alone security solutions to varying attacks at different layers with peculiar objectives the crux is that security objectives in CR/ CRN domain should unfold in a systematic manner to make it easier on the CR and reduce the undue processing overhead whereby making it an efficient process. How should this unfold? Prime most priority goes to Identity which is the basis for authentication based on which secondary users (SU) are segregated from primary users (PU) and which results in authorization based on their identities as we clearly understand that PU and SU merit distinct rights. Implying Identification, Authentication and Authorization are key to smooth functioning of the CR environment.

Identity fabrication leads to Sybil Attacks that in turn builds the basis of intelligent malicious activity which when successful forms the launching pad for further insider attacks (sinkhole, wormhole, HELLO) across traditional/ CR NWs and PUEA , SSDF (vulnerability which leads to OFA, CAA etc) in Cognitive Radio networks. Any solution of filtering out attackers in CR/ CRN if it kick starts with correctly identifying identities (filtering Sybil attack) it will start having a corrective ripple effect of implicitly resolving insider attacks and further paving way for addressing CR/ CRN specific attacks. Hence, having drawn a line between Internal and External entities plus filtering legitimate identities the issues left would be any internal authenticated identity performing a selfish or malicious act which would be either for personal gain or to bog

down the NW respectively. If thought over systematically it brings us down to the fact that in a CR environment secondary user (SU) would back off from licensed bandwidth in presence of a primary user (PU); so if a con node/ malicious secondary user (MU) portraying itself as a primary user in other words emulating as a primary user can be sorted out/ filtered then the only issue left would be authenticated authorized entities in the CR eco system with the dilemma of a malicious secondary user trying to intelligently gain complete access of the vacant spectrum without equilibrium in co-existence with other SU or initiating communication during primary user transmissions resulting in collisions and legal issues for CRN operator. If this last hurdle of false sensing data transmission is filtered out a clean CR/ CRN eco system is available.

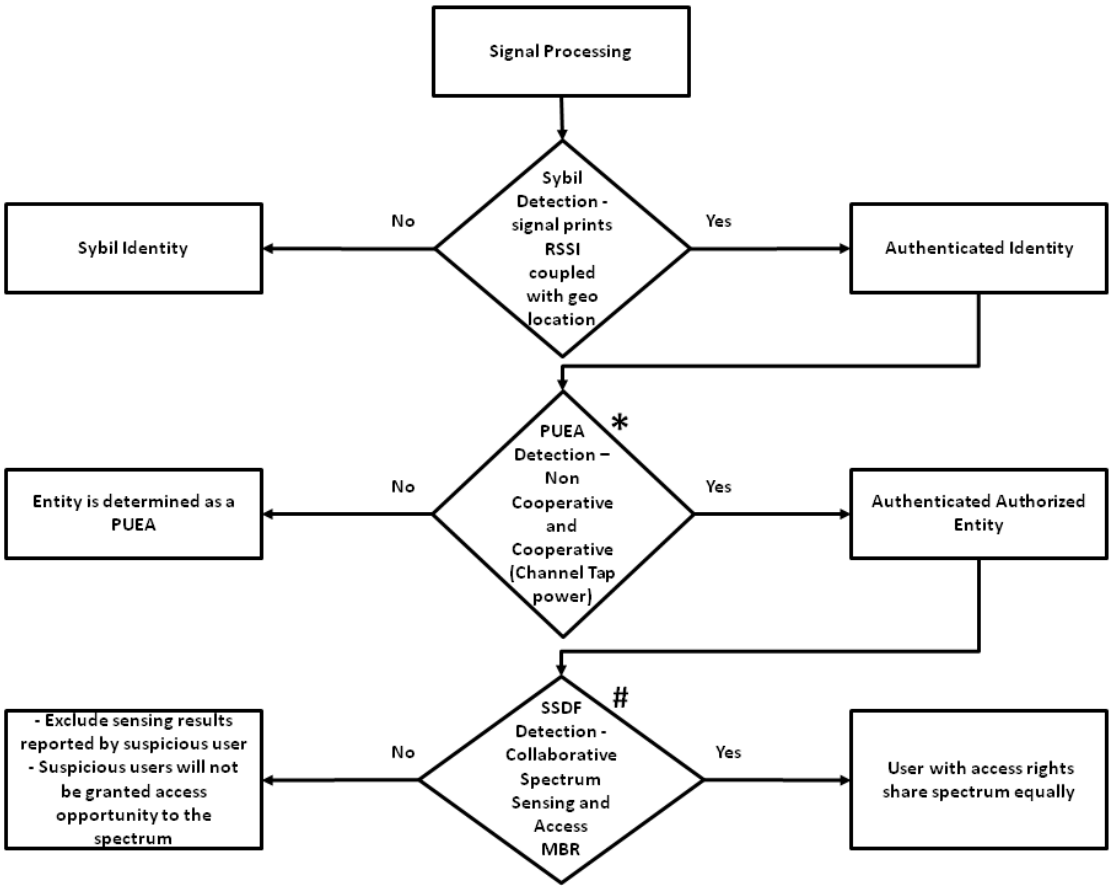

Figure 5.1: Security Model

For all these reasons; therefore, a security model/ comprehensive framework as depicted in figure 5.1 may be constituted for a CR/ CRN based on a step by step oper-

ational flow and amalgamation of the stand alone efficient solutions currently proposed till date. The operational flow should start off by addressing Sybil attack followed by PUEA and then SSDF which would implicitly sort out insider threats (sinkhole, wormhole, HELLO) and threats to the Cognitive nature (OFA, CAA, RIJ etc) of the CRN. This security model would be more pertinent and beneficial in an IEEE 802.22 WRAN environment where the secondary user will all employ standard HW for connectivity to BS/FC for provision of broadband services on longer range in sparsely populated rural areas employing TV broadcast band whitespaces. The BS/ FC will be in knowledge of the PU which are the TV broadcast towers/ HW serving that geographical area and the SU which are the customer premises equipment in its service radius as the draft standard of IEEE 802.22 puts it "All devices in the network to be installed in a fixed location and the BS is required to know its location and the location of all of its associated CPEs and incumbent services". This requirement is met by, equipping all SU in the CRN with GPS and access to a DB with information about entities in the geographical area to include SU and up-to-date and accurate information of PU, auxiliary low-power licensed operations and other IEEE 802.22 operations in the area.

Solution employed for Sybil attack in the model maybe crafted on signal prints based on RSSI coupled with geo location which serve the purpose because a transmiter can be uniquely identified on base of signalprints that are unique based on a location.

Protection against PUEA in the model maybe based on the channel tap power that can serve as a fingerprinting mechanism of radio frequency to directly detect PUEA through a non-collaborative and collaborative mechanism as depicted in the figure 5.2. The technique has the advantage of detection in Rayleigh environments (shadowing, fading and low sound to noise ratio (SNR)) under Doppler effects reducing false positive to approximately zero [76].

Protection against SSDF in the model maybe based on malicious behaviour resistance which employs collaborative optimized spectrum sensing and access data as

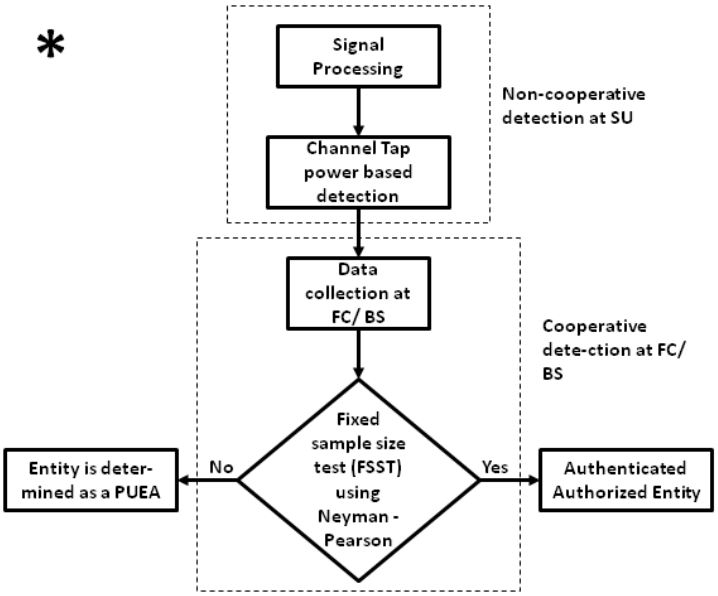

Figure 5.2: PUEA Detection Model

depicted in the figure 5.3. The technique has the advantage of combining sensing and access data for prevention rather than standalone which drastically reduces false alarms, curbing the malicious user intelligent behaviour of out of the box actions rather than deterministic malicious behaviour alone [77].

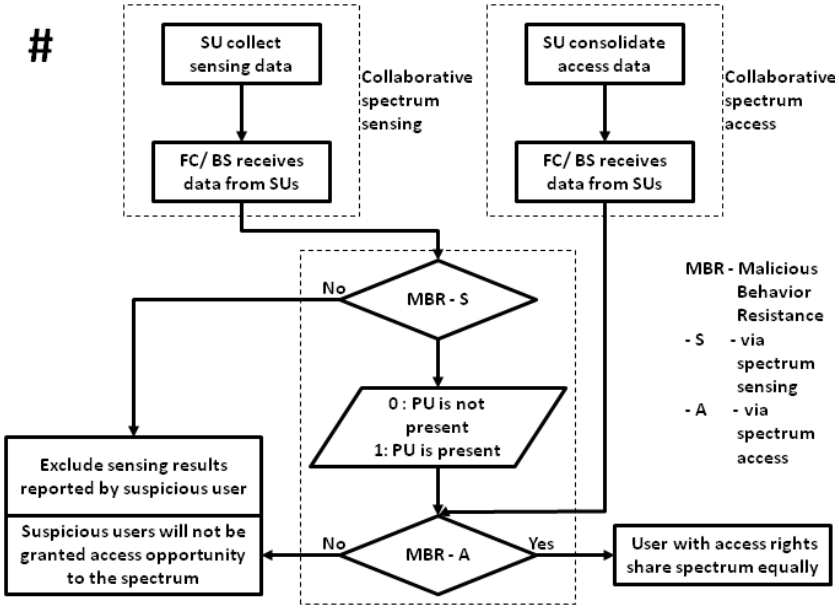

Figure 5.3: SSDF Detection Model

Chapter 6

CONCLUSION

6.1 Conclusion

Spectrum Availability is a major issue of the new era as spectrum space has almost been exhausted by years of implementation of the static spectrum allocation policies. CR - a promising concept that sprouted gave a breathing space to spectrum planners as opportunistic spectrum deployment and utilization was revolutionized by this concept. CRN is the evolution of wireless communication. The potentials of CRN are limitless, the most fascinating phenomenon materializing within the wireless communication domain. Security is a cornerstone of any technology and needless to say it holds true in the CR domain as well. Security is an issue of grave alarm vis-à-vis CRN based on their intrinsic characteristics which opens them up to a load of vulnerabilities.

Protecting the priority of usage for PU is the daunting task in CRN. Hence, attacks of all creed, make and type have attracted significant recognition in CRN. As security has high precedence in CRN, major threats were consolidated to comprehend the environment concerning CRN. In this work, CRN has been discussed, explained and analyzed from security angles. Deployment and performance considerations were discussed that are threatened by these vulnerabilities. Various challenges vis-à-vis security concerns are described with a view to encourage areas for improvement, optimization

and deployment of new solutions to address issues pertaining to CRN. This work has enlisted vulnerabilities to CRN by delineating attacks based on layers. Moreover, consolidation of solutions for security at different layers has been presented i.e. Attack countermeasures / Attack mitigation techniques were consolidated. New avenues for further improvement on these techniques and innovating with new solutions are wide open.

6.2 Future Work

CRN is an evolving technology in terms of optimized communication, protocols, standards and security solutions. Unlike regular communication networks, CRN ecosystem is constrained in terms of bandwidth capacity, sensing, processing, adaptation and action (power output) due to which implementation of traditional security mechanism applicable in distributed ad-hoc NW are challenging and difficult. Research community all around the world is contributing to address issues and security concerns in CRN domain. Meanwhile, several challenges still remain for CRN which merits research and development to reap potential benefits of CRN technology. Hence, CRN is a domain where various research areas are open and many of the researches are in full swing to address challenges for the success of CRN.

In this research, various aspects of CRN have been studied, enlisted and consolidated. It is expected that consolidation of security aspects of deployment and communication approaches can contribute towards research community who are interested to optimize, improve or develop new solutions by addressing security concerns in CRN. Moreover, before CRN standardization points enlisted in this work can be explored. As standardization contribute towards success of any technology; therefore, different vulnerability aspects described and analyzed in this work can be addressed for further improvement of CRN. Finally, tabular reckoners have been presented which can be evaluated and experimented for improvement in CRN.

References

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13-18, 1999.

[2] 802.22 Working Group, "IEEE 802.22 D1: draft standard for wireless regional area networks," March 2008, http://grouper.ieee.org/groups/802/22/.

[3] C. Stevenson, G. Chouinard, Z. D. Lei, W. D. Hu, S. Shellhammer and W. Caldwell, "IEEE 802.22: the first cognitive radio wireless regional area network standard," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 130-138, Jan. 2009.

[4] Wireless Innovation forum http://www.wirelessinnovation.org/.

[5] Y. Zeng, Y.-. Liang, A.T. Hoang and R. Zhang, "A review on spectrum sensing for cognitive radio: challenges and solutions," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, Article 2, Jan. 2010.

[6] T. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multidimensional analysis and assessment," *Mobile Network Application*, vol. 13, no. 5, pp. 516-532, Oct. 2008.

[7] M. Sherman, A. N. Mody, R. Martinez, C. Rodriguez and R. Reddy, "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence," *IEEE Communications Magazine*, vol. 46, no. 7, pp. 72-79, Jul. 2008.

[8] A. N. Mody, M. J. Sherman, R. Martinez, R. Reddy and T. Kiernan, "Survey of IEEE standards supporting cognitive radio and dynamic spectrum access," *MILCOM 2008 - 2008 IEEE Military Communications Conference*, San Diego, CA, pp. 1-7, 2008.

[9] X Max Spectrum Crisis Solutions® xG Technology Inc® (2014,June,12)[Online]. Available: http://www.xgtechnology.com/Technology/Cognitive-Radio-Network.html.

[10] K. Tan, S. Jana, P.H. Pathak and P. Mohapatra, "On insider misbehavior detection in cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 4-9, May-June 2013.

[11] M. Padmadas , N. Krishnan and V.N. Nayaki, "Analysis of Attacks in Cognitive Radio Networks," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 8, Aug. 2015.

[12] M. José, J. Granjal and E. Monteiro, "A survey on security attacks and countermeasures with primary user detection in cognitive radio networks," *EURASIP Journal on Information Security*, vol. 2015, no. 1, Apr. 2015.

[13] D. Das and S. Das, "Primary User Emulation Attack in Cognitive Radio Networks: A Survey," *IRACST - International Journal of Computer Networks and Wireless Communications (IJCNWC)*, vol. 3, no. 3, Jun. 2013.

[14] R. Dubey, S. Sharma and L. Chouhan, "Secure and trusted algorithm for cognitive radio network," *2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN)*, Indore, pp. 1-7, 2012.

[15] Internet World Stats © Miniwatts Marketing Group (2017,December,31)[Online]. Available: http://www.Internetworldstats.com/stats.htm.

[16] A.M. Hayar, R. Pacalet and R. Knopp, “Cognitive radio Research and Implementation Challenges,” *2007 Conference Record of the Forty-First Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, pp. 782-786, 2007.

[17] X. Zhou, K. Yazdandoost, H. Zhang and I. Chlamtac, “Cognospectrum: Spectrum adaptation and evolution in cognitive ultra-wideband radio,” *2005 IEEE International Conference on Ultra-Wideband*, Zurich, pp. 713-718, Sep. 2005.

[18] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[19] P. Steenkiste, D. Sicker, G. Minden and D. Raychaudhuri, “Future Directions in Cognitive Radio Network Research,” *NSF Workshop Report*, 2009.

[20] R.K. Sharma and D. B. Rawat, “Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 1023-1043, Secondquarter 2015.

[21] M. Haddad, A.M. Hayar, M.H. Fetoui and M. Debbah, “Cognitive Radio sensing based on information-theoretic,” *CrownCom 2007 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Orlando, FL, pp. 241-244, 2007.

[22] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran and S. Mohanty, “A survey on spectrum management in cognitive radio networks,” *IEEE Communication Magazine*, vol. 46, no. 4, pp. 40-48, Apr. 2008.

[23] IEEE Std 802.22™-2011, IEEE Standard for Wireless Regional Area Networks.

[24] K.-C. Chen, Y.-J. Peng, N. Prasad, Y.-C. Liang and S. Sun, “Cognitive radio network architecture: part 1 general structure,” *Proceedings of the 2nd Inter-*

national Conference on Ubiquitous Information Management and Communication(ICUIMC '08), Suwon, ACM, New York, NY, pp. 114-119, 2008.

[25] S. Haykin, "Fundamental issues in Cognitive Radio," *Hossain E. and Bhargava V. (eds) in Cognitive Wireless Communications Networks*, Springer-Verlag, Boston, MA, pp. 1-43, 2007.

[26] E. Hossain and K.G.M. Thilina, "Cognitive radio networks and spectrum sharing," *Academic Press Library in Mobile and Wireless Communications*, Elsevier, pp. 467-522, 2016.

[27] J. Agarkhed and V. Gatate, "Survey on spectrum sensing techniques in cognitive radio networks," *International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, pp. 1440-1445, 2017.

[28] Federal Communications Commission (FCC), "Facilitating opportunities for flexible, efficient and reliable spectrum use employing spectrum agile radio technologies," *ET Docket No.03-108*, December 2003.

[29] IETF RFC 2026 (1996,October,30)[Online]. Available: http://tools.ietf.org/html/rfc2026.

[30] Qusay H. MAHMOUD, "Cognitive Networks: Towards Self-Aware Networks," John Wiley and Sons, London, 2007.

[31] C.N. Mathur and K.P. Subbalakshmi, "Security Issues in Cognitive Radio Networks," *Cognitive Networks: Towards Self-Aware Networks*, Wiley-Blackwell, New York, NY, pp. 271-291, 2007.

[32] L. Hou, K.H. Yeung and K.Y. Wong, "A virus spreading model for cognitive radio networks," *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 24, pp. 6632-6644, 2012.

[33] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks : Attacks and Countermeasures," *First IEEE International Workshop on Sensor Network Protocols and Applications*, Anchorage, AK, pp. 113-127, 2003.

[34] A. Attar, H. Tang, A.V. Vasilakos, F. Richard Yu and V.C.M. Leung, "A survey of security challenges in cognitive radio networks: solutions and future research directions," *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172-3186, Dec. 2012.

[35] Y. Tan, K. Hong, S. Sengupta and K.P. Subbalakshmi, "Spectrum stealing via Sybil attacks in DSA networks: implementation and defense," *IEEE International Conference on Communications(ICC)*, Kyoto, pp. 1-5, Jun. 2011.

[36] S. Misra, A. Ghosh, A.P. Sagar and M.S. Obaidat, "Detection of identity-based attacks in wireless sensor networks using signal prints," *IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, GreenCom 2010, Hangzhou, pp. 35-41, 18-20 Dec. 2010.

[37] L. Ma, C. Shen and B. Ryu, "Single radio adaptive channel algorithm for spectrum agile wireless adhoc networks," *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN 2007)*, Dublin, pp. 547-558, 2007.

[38] A. Popescu, "Cognitive radio networks," *2012 9th International Conference on Communications (COMM)*, Bucharest, pp. 11-15, 2012.

[39] A. Sampath, H. Dai, H. Zheng and B.Y. Zhao, "Multi-channel Jamming Attacks Using Cognitive Radios," *2007 16th International Conference on Computer Communications and Networks*, ICCCN 2007, Honolulu, HI, pp. 352-357, Aug. 2007.

[40] W. Xu, T. Wood, W. Trappe and Y. Zhang, "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service," *3rd ACM Workshop on Wireless Security (WiSe '04)*, ACM, New York, NY, pp. 80-89, 2004.

[41] T.C. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, Singapore, pp. 1-8, May 2008.

[42] S.T. Zargar, M.B.H. Weiss, C.E. Caicedo and J.B.D. Joshi, "Security in Dynamic Spectrum Access Systems: A Survey," *working paper. UNSPECIFIED*, University of Pittsburgh, 2011, http://d-scholarship.pitt.edu/2823/.

[43] S. Misra, S.S. Chatterjee and M. Guizani, "Stochastic learning automata-based channel selection in cognitive radio/dynamic spectrum access for WiMAX networks," *International Journal of Communication Systems*, vol. 28, no. 5, pp. 801-817, Mar. 2015.

[44] A. Naveed and S.S. Kanhere, "NIS07-5: Security Vulnerabilities in Channel Assignment of Multi-Radio Multi-Channel Wireless Mesh Networks," *Global Telecommunications Conference IEEE GLOBECOM 2006*, San Francisco, CA, pp. 1-5, 2006.

[45] W. Wang, Y. Sun, H. Li and Z. Han, "Cross-Layer Attack and Defense in Cognitive Radio Networks," *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, Miami, FL, pp. 1-6, Dec. 2010.

[46] H.P. Patel and M.B. Chaudhari, "Survey: impact of jellyfish on wireless adhoc network," *International Journal of Engineering Research and Technology(IJERT)*, vol. 1, no. 9, Nov. 2012.

[47] J. Hernández-Serrano, O. León and M. Soriano "Modeling the Lion Attack in

Cognitive Radio Networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, article no. 2, pp. 2:1-2:10, Jan. 2011.

[48] L. Qian, X. Li and S. Wei, "Cross-layer detection of stealthy jammers in multihop cognitive radio networks," *2013 International Conference on Computing, Networking and Communications (ICNC)*, San Diego, CA, pp. 1026-1030, 2013.

[49] J.R. Douceur, "The Sybil attack," *1st International Workshop on Peer-to-Peer Systems IPTPS 2002*, Cambridge, MA, Lecture Notes in Computer Science, vol. 2429, Springer, Berlin, Heidelberg, pp. 251-260, Mar. 2002.

[50] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil attack in sensor networks: analysis & defenses," *3rd International Symposium on Information Processing in Sensor Networks (IPSN '04)*, Berkeley, CA, ACM, New York, NY, pp. 259-268, Apr. 2004.

[51] L. Xiao, W. S. Lin, Y. Chen and K.J.R. Liu, "Indirect reciprocity game modeling for secure wireless networks," *2012 IEEE International Conference on Communications (ICC)*, Ottawa, ON, pp. 928-933, Jun. 2012.

[52] S Bhattacharjee, S. Sengupta, and M. Chatterjee, "Vulnerabilities in cognitive radio networks: A survey," *Computer Communications*, vol. 36, no. 13, pp. 1387-1398, Jul. 2013.

[53] A.S. Rawat, P. Anand, H. Chen and P.K. Varshney, "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774-786, Feb. 2011.

[54] W. Wang, H. Li, Y. Sun and Z. Han, "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks," *2009 43rd Annual Conference on Information Sciences and Systems (CISS 2009)*, Baltimore, MD, pp. 130-134, Mar. 2009.

[55] L. Lu, S.Y. Chang, J. Zhang, L. Qian, J. Wen and V.K.N. Lau, "Technology Proposal Clarifications for IEEE 802.22 WRAN Systems," *IEEE 802.22 WG on WRANs*, Mar. 2006.

[56] P. Kaligineedi, M. Khabbazian and V.K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," *2008 IEEE International Conference on Communications (ICC '08)*, Beijing, pp. 3406-3410, May 2008.

[57] A. Pandharipande, J.-M. Kim, D. Mazzarese, and B. Ji, "IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22," *IEEE 802.22 WG on WRANs*, Nov. 2005.

[58] J. Hillenbrand, T.A. Weiss and F.K. Jondral, "Calculation of Detection and False Alarm Probabilities in Spectrum Pooling Systems," *IEEE Communication Letters*, vol. 9, no. 4, pp. 349-351, Apr. 2005.

[59] A. S. Rawat, P. Anand, H. Chen and P.K. Varshney, "Countering Byzantine Attacks in Cognitive Radio Networks," *2010 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Dallas, TX, pp. 3098-3101, Mar. 2010.

[60] R. Chen, J. Park, Y.T. Hou and J.H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 50-55, Apr. 2008.

[61] K. Bian and J. Park, "MAC-Layer Misbehaviors in Multi-hop Cognitive Radio Networks," *2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006)*, pp. 228-248, Aug. 2006.

[62] L. Lazos, S. Liu and M. Krunz, "Mitigating control channel jamming attacks in multichannel ad hoc networks," *Second ACM Conference on Wireless Network Security (WiSec '09)*, Zurich, ACM, New York, NY, pp. 169-180, Mar. 2009.

[63] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '05)*, Urbana-Champaign, IL, ACM, New York, NY, pp. 46-57, May 2005.

[64] A. Khare, M. Saxena, R.S. Thakur and K. Chourasia, "Attacks & Preventions of Cognitive Radio Networks-A Survey," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 2, no. 3, Mar. 2013.

[65] O. León, J. Hernández-Serrano and M. Soriano, "Securing Cognitive Radio Networks," *International Journal of Communication Systems*, vol. 23, no. 5, pp. 633-652, May 2010.

[66] Q. Yan, M. Li, T. Jiang, W. Lou and Y.T. Hou, "Vulnerability and protection for distributed consensus based spectrum sensing in cognitive radio networks," *2012 Proceedings IEEE INFOCOM*, Orlando, FL, pp. 900-908, Mar. 2012.

[67] K. Lu, H. Ke, J. Yang and L. Zhang, "Research of PUE attack based on location," *2012 IEEE 11th International Conference on Signal Processing (ICSP)*, Beijing, pp. 1345-1348, Oct. 2012.

[68] X. Zheng, Y.Li and H. Zhang, "A collision free resident channel selection based solution for deafness problem in the cognitive radio networks," *2010 IEEE International Conference on Wireless Information Technology and Systems (ICWITS)*, Honolulu, HI, pp. 1-4, Aug. 2010.

[69] A.L. Toledo and X. Wang, "Robust detection of selfish misbehavior in wireless networks," *IEEE Journal on Selected Areas in Communications*, Vol. 25, No. 6, pp. 1124-1134, Aug. 2007.

[70] Y. Zhang and L. Lazos, "Vulnerabilities of cognitive radio MAC protocols and countermeasures," *IEEE Network*, vol. 27, no. 3, pp. 40-45, May-June 2013.

[71] F. Samad, Q.A. Ahmed, A. Shaikh and A. Aziz, "JAM: Mitigating Jellyfish Attacks in Wireless Ad Hoc Networks," *International Multi Topic Conference IMTIC 2012 - Emerging Trends and Applications in Information Communication Technologies*, Jamshoro, Mar. 2012, Communications in Computer and Information Science, vol. 281, Springer, Berlin, Heidelberg, pp. 432-444, 2012.

[72] A.A. Pirzada and C. McDonald, "Trust establishment in pure ad hoc networks," *Wireless Personal Communications*, vol. 37, no. 1-2, pp. 139-168, Apr. 2006.

[73] N. Jiang, K.A. Hua and D. Liu, "A scalable and robust approach to collaboration enforcement in mobile ad-hoc networks," *Journal of Communications and Networks*, vol. 9, no. 1, pp. 56-66, Mar. 2007.

[74] O. León, J. Hernández-Serrano and M. Soriano, "A new cross-layer attack to TCP in cognitive radio networks," *2009 Second International Workshop on Cross Layer Design (IWCLD '09)*, Palma de Mallorca, pp. 1-5, Jun. 2009.

[75] T. Goff, J. Moronski, D.S. Phatak and V. Gupta, "Freeze-TCP: a true end-to-end TCP enhancement mechanism for mobile environments," *IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064)*, Tel Aviv, Vol. 3, pp. 1537-1545, Mar. 2000.

[76] T. N. Le, W. Chin and Y. Lin, "Non-cooperative and cooperative PUEA detection using physical layer in mobile OFDM-based cognitive radio networks," *2016 International Conference on Computing, Networking and Communications (ICNC)*, Kauai, HI, 2016, pp. 1-5, Feb. 2016.

[77] W. Wang, L. Chen, K. G. Shin and L. Duan, "Secure cooperative spectrum sensing and access against intelligent malicious behaviors," *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, Toronto, ON, 2014, pp. 1267-1275, Apr. 2014.