International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue1 | ISSN : 2456-3307

Study of Attacks and their Defence Methods in CRN: A Survey

Aasia Rehman*[1], Deo Prakash[2]

*[1]Lecturer, P.G Department of Computer Science in Kashmir University, Srinagar, J&K, India
Aasiya.rehman77@gmail.com[1]
[2]Assistant Professor, Department of CSE in SMVD University, India
Dev.smvdu@gmail.com[2]

ABSTRACT

Cognitive Radio Technology is considered as a developing technology in which wireless nodes are skilled in such a way that they can change their transmitting parameters dynamically as per the sensed data from the radio spectrum to utilize the deficient spectrum in an efficient and promising way. Although CRN can improve the overall network performance but it is susceptible to a number of security attacks due to its flexibility and disclosed wireless nature. The various attacks on CRN have been classified as physical layer, MAC layer, network layer, transport layer attacks, application layer attacks and cross layer attacks. This paper provides the introduction to CRN, its working process, Architecture of CRN, Cognitive Radio Engine Architecture, various classes of Attacks and their defence methods.

Keywords : CRN, RF, FCC, Cognitive Radio, Cognitive Radio Networks, Jamming, Primary User Emulation Attack, Dynamic Spectrum Access

I. INTRODUCTION

In cognitive radio networks secondary users or Cognitive Radios dynamically senses for white spaces in the licensed band using spectrum sensing algorithms and uses them for communication purposes. In other words Cognitive Radio in CRN is a radio that senses the spectrum band for free channels and then adapts its transmitting parameters (modulation type, frame size, operating frequency, transmitting power etc.) according to the environment to allow concurrent wireless communication through the same frequency band [1]. We have two different types of cognitive radio nodes: the policy radios and the learning radios [2].

- ✓ Policy Radios detect the behavior of the cognitive radio by analyzing some predefined policies. When the environment is sensed, the radio collects the data from the environment and then extracts useful information from it which we called statistics which in turn gives the state of the radio.
- ✓ Learning Radios in addition have a learning engine that is used to arrange and rearrange the states of the radios.

To distinguish CR from the traditional radios, CR has novel radio frequency transceiver architecture [3]. The important parts of transceiver are as shown in the Figure 1 [4] the RF front end which consists of Radio Frequency and Analog-to-Digital converter, and a Baseband processing. Both the parts are reconfigured through a control bus to re-adjust according to the changing RF-environment. The received signal is amplified, mixed and analog-to-digital converted in the RF front end unit. Next the signal is modulated or demodulated and encoded or decoded in the Baseband processing unit. The most important feature of the CR transceiver is the ability of the RF front end to perform wideband sensing. This ability of RF front end is mainly concerned with

the RF hardware technologies e.g. wideband antenna, power amplifier, Mixer, Voltage-controlled oscillator (VCO) and adaptive filter. RF hardware should be able to tune to any portion of the spectrum band.

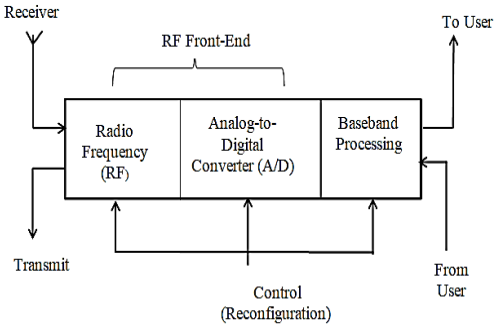

Figure 1. CR Transceiver

Cognitive Radio networks: CRN network is formed by putting together several CR's (unlicensed users) to construct a network together with the legitimate users of the spectrum band. The cognitive radio in CRN is a device that first senses the surroundings i.e. environment and then trains from it and reconfigure its internal framework as per the data that is sensed.

It has two main goals robust communication anywhere and anytime and valuable use of the available frequency spectrum.

The term Cognitive Radio was first introduced by Mitola in 2000 as an extension to software defined radio (SDR) [5]. The primary intension was to efficiently utilize the spectrum band. With the increase in the number of wireless networks in the internet the need for spectrum also increases rapidly and hence there is the scarcity of frequency bands for these networks or applications. The main idea was to develop an intelligent agent embedded in lightweight equipment's like PDA's to accomplish the basic transmission requirements of the user. Use of vacant frequency bands or vacant channels in the spectrum band anywhere anytime is referred to as Dynamic Spectrum Access (DSA) [6] [3][1]. As a result of this the Federal Communications Commission (FCC) allowed the use of certified spectrum by the prohibited users. Thus the unlicensed users can utilize the free spectrum but it should not intervene with the primary users. The problem of spectrum shortage was reduced due to the cognitive radio technology.

1.1 Working Process of CRN

A CRN have four main working functionalities as shown in Figure 2.

i. Cognitive Ability
ii. Self-concerned Ability
iii. Decision capability
iv. Reconfigurable capability

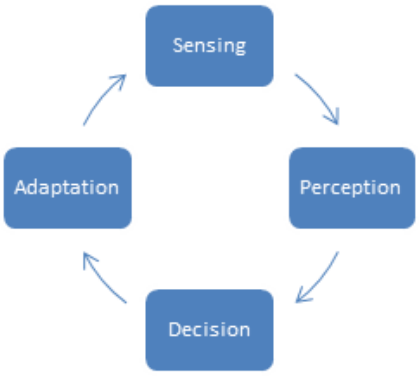

Figure 2.working process of CR

i. Cognitive Ability [5]: The CR networks have the ability of sensing the spectrum and determine if there are any spectrum holes available in the network. If the spectrum holes are detected then the unauthorized users uses that band for communication causing less intrusion for licensed users. Various algorithms are used for sensing the spectrum. The CR also enables spectrum sharing, location recognition, network detection and service detection.
ii. Self-organize Ability [5]: A CR in CRN should collaborate and self-organize so as to produce efficient performance of the network by allowing the operation of only those CR nodes which are needed while disabling those nodes which are not needed for communication.
iii. Decision capability [5]: The CRN needs to decide on the use of resources that are shared, a modification in parameters and nodes configuration etc.

iv. Reconfigurable capability [5]: There are various reconfigurable abilities of CRNs some of them are as: Frequency agility, Dynamic frequency selection, Adaptive modulation, Power change, Access to dynamic networks.

II. CRN ARCHITECTURE

There are 3 prime architectures of CRNs [5]. The elementary parts of each of the architectures are Base Stations, Mobile stations and the backbone architecture [5]. These 3 architectures are as under:

1.2 Infrastructure architecture:

In infrastructure architecture as shown in Figure 3 each mobile station are able to contact with other mobile station only if both of them are under the area of same base station. The services of each CR are explained in advance in this type of architecture. It is centralized architecture with a central base station. The data collected by every CR device is transferred towards the prime base station.

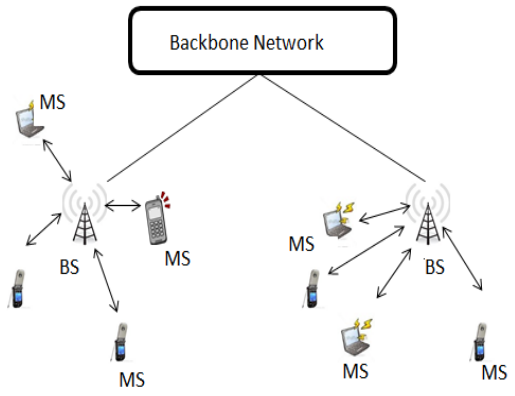

Figure 3. Infrastructure Architecture

2.2 Ad hoc architecture:

Ad hoc has no backbone network base as shown in Figure 4. The mobile station watches its environment to detect if there are few mobile stations that can be connected by using protocols then they are joined by a communication link thus it forms ad hoc architecture. Thus the nodes are linked via an ad hoc contact on both authorized and unauthorized frequency bands. In this type each CR node has all the abilities and can predict the next level in an affair using the local information that it obtained during observation. This local information is not ample for determining the effect of its behavior on the network due to which co-operative techniques are useful where this locally observed information is shared with other nodes to widen the capability of the whole CR network.

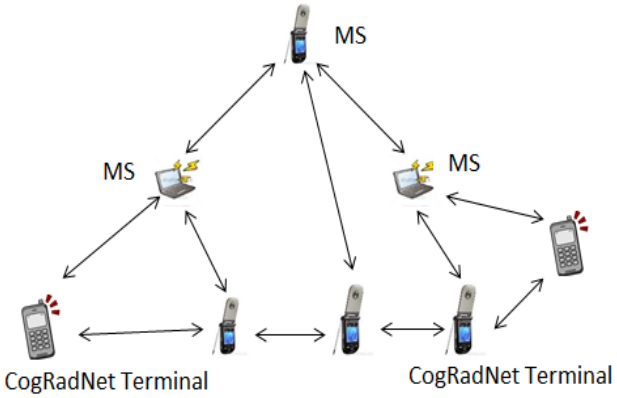

Figure 4. Adhoc Architecture

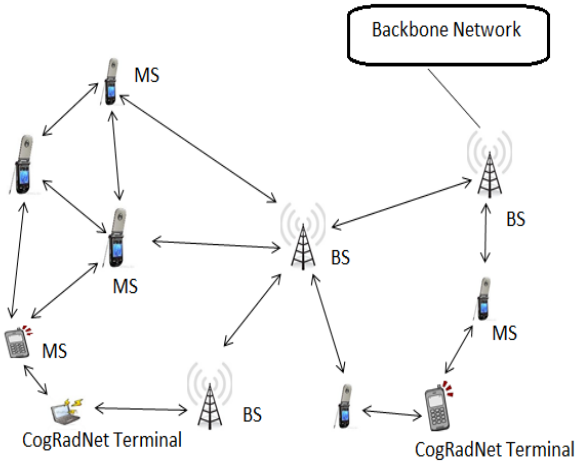

Figure 5. Mesh Architecture

2.3 Mesh architecture:

The Mesh architecture is a mix of both infrastructure as well as ad hoc architecture as shown in Figure 5. The Base station is linked to others through wireless connections. They form the basis for the mesh architecture. Mobile stations are joined to base station either directly or via several mobile stations. It has the supremacy and limitations of both the architectures.

III. CRN FUNCTIONS AND THEIR CHALLENGES

The various functions performed by cognitive radio network and their challenges are as under:

3.1 Spectrum sensing:

Sensing the spectrum is necessary requisite for making CRN realistic. A CR node should know about the modification in its environment [5]. Spectrum sensing makes cognitive radios to reconfigure themselves as per the surrounding by identifying the band holes not causing any disturbance to licensed users.

Challenges:

- ✓ Measurement of Interference: A CR does not completely know the position of primary receivers due to the weak inter-communication among primary users and CRs. Therefore modern methods are needed to determine the interference measurement at the primary networks [5].
- ✓ Multi-user network spectrum sensing: In case of multiple secondary users and primary users it becomes more complex to sense the bands and measure interference. Thus new efficient procedures need to be built for band sensing in case of multi user networks [5].
- ✓ Efficient spectrum sensing: The cognitive radio is not able to implement both sensing and transmit data simultaneously. It is known as sensing efficiency problem. As a result transmitting should not take place while sensing the spectrum. Also specific algorithms must be developed so that the time to sense the spectrum should be reduced under the sensing preciseness [5].
- ✓ Covered Primary user problem: Here CR users affect the licensed users because the primary signal cannot be identified due to its position [5].

3.2 Decision about spectrum: Once the spectrum has been sensed CRN requires deciding among various spectrum bands that are available, which one is most suitable one to be used for communication based on quality of service specific to the function.

Challenges:

- ✓ Reconfigure: The methods of cognitive radio networks reconfigures the certain features of transportation for the ideal performance in a specific spectrum [5].
- ✓ Decision of spectrum band between dissimilar bands: A CRN needs to perform spectrum selection process in authorized as well as unauthorized spectrum [5].

3.3 Sharing of Spectrum: Sharing spectrum involves 2 categories: sharing within the same cognitive radio network and sharing between different cognitive radio networks.

Challenges:

- ✓ CCC (common control channel): CCC is useful in sharing of spectrum performance. Howeverits application is impractical for the reason that it should be relinquished at any time when the primary user selects it [5].
- ✓ Dynamic Radio range: The operational frequency of CRs is usually modified due to dependency among operational frequency and range of radio. Till now no task has been done to overcome this problem [5].
- ✓ Knowledge of Position: Unauthorized users are constantly instructed about the licensed user's position and energy. This knowledge about the primary user's position is used to validate every user in order to give security and authentication in networks [5].

3.4 Mobility of spectrum:

The mobility of spectrum means frequency hand off when a PU becomes active in the licensed band which is occupied by the secondary users then the secondary user needs to move from one spectrum to another that is not used. This step is to ensure the stable interaction at the time of hand off of spectrum bands.

Challenges:

- ✓ Time domain mobility: Based on the possibility of unused spectrum bands CRN adapts to the band. Due to the changing nature of the unused spectrum bands the quality of service here has turn out to be a threat [5].
- ✓ Space mobility: As the secondary users shift from point to point over time the presence of accessible bands also switches over time. Thus regular allotment of unused bands in these networks is a challenging problem [5].

IV. COGNITIVE RADIO ENGINE ARCHITECTURE

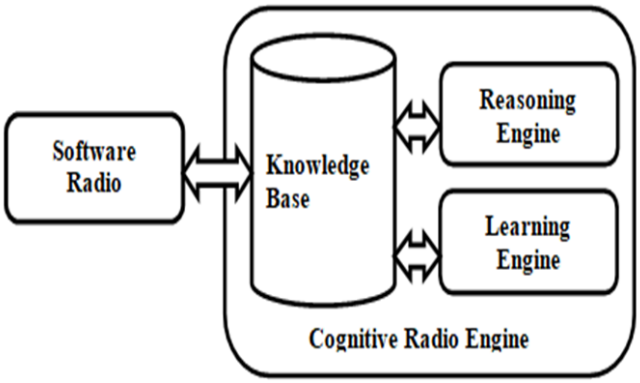

Figure 6. CRN Engine Architecture

Cognitive radio consists of 4 main parts as: Software defined radio, knowledge base, reasoning engine, learning engine [7] as shown in Figure 6. SDR is a device that can be highly configured. It has leading end that can be adjusted to different frequencies and it also has an amplifier which permits interaction at various levels of power. A modem can apply different modulation techniques. It also has a number of input sensors that can accept digital RF input and provide significant outcomes. E.g. an energy detector can calculate the power that is received at a certain frequency to indicate if the band is already in use or not. There are also number of receiver sensors that can be used to figure out signal to noise ratio, bit error rate and frame error rate. The SDR interface introduces these input and output sets to a controlling entity which chooses a collection of inputs and produces a set of optimal outputs which is defined by objective function. Inputs are chosen by an optimization problem which is handled by cognitive engine. The inputs are given to the engines, knowledge base as read-only data or read-write data. The knowledge base consists of a collection of intelligent explanations that denotes the radios state. The cognitive engine consists of two engines the reasoning and the learning engine. Reasoning engine is present in both policy radios and learning radio whereas learning engine is present only in learning radio. There are reasoning rules in the reasoning engine to which a collection of actions, circumstances in which these action are executed, and also by virtue of what the state of knowledge base is affected by these actions. In case of learning radios the learning engine tries all possible configurations in order to view how the CR reacts to them. They use algorithms like AI, search, neural networks and evolutionary. A cognitive radio works on the basis of a cognitive cycle as Observe, orient, plan, decide and act and incase of learning radio extra step is added i.e. learn [8]. In attacking the CRs the intruder needs to operate on observe step and rest will be affected automatically.

V. SPECTRUM SENSING

Spectrum sensing is one of the essential tasks of a CR node. The primary objective of spectrum sensing is to identify the holes in the spectrum and primary users in licensed spectrum band. A CR node senses the surrounding environment for the availability of the spectrum holes in the particular frequency band then utilizes these spectrum holes for the efficient communication and also leaves the spectrum immediately whenever a PU is identified so that no obstruction is caused to primary system. The most important challenging issue for CR node in spectrum sensing is making sure that the sensing results are error free that may occur due to the hidden node problem. This issue is removed to some extent in distributed spectrum sensing; where every CR node performs the local spectrum sensing and sends the sensed outcome to the data collector which with the help of several methods produces the final results of sensing. Spectrum sensing techniques are grouped into 3 classes as shown in Figure 7 [9]: Non-cooperative sensing, Cooperative sensing, Interference sensing.

5.1 Non-cooperative sensing:

It is also known as transmitter detection technique [9]. It is further divided as energy detection [15], matched filter detection and Cyclo-stationary feature methods [15]. In energy detection primary user is sensed according to detected energy. This is the easiest method and it does not depend on any previous data of PU system. Energy detection is the most widely used method for spectrum sensing [10][11]. In this method the energy of the entering signal is co-related with a predetermined threshold to detect the primary signal. The matched filter method decides the existence of licensed users by analyzing the signal to noise ratio. The fundamental limitation of the matched filter is that it depends upon the prior awareness of the primary system signal features. Cyclo-stationary feature detection method works by detecting the existence of primary system by analyzing the low signal to noise ratio. Cyclo-Stationary is the most complex method. It also needs former awareness of the primary signal. Here the signal is first sampled and then its amplitude is normalized. The peak value of amplitude is compared with the predefined threshold if periodicity is detected then the band is occupied by the primary signal. Otherwise band is free to be used.

5.2 Cooperative Sensing:

It is also divided into 3 categories [9] Centralized Coordinated, Decentralized Coordinated and Decentralized Uncoordinated [12] [13]. In centralized coordinated, a CR node performs sensing to reveal the existence of primary transmitter or receiver and sends the sensed data to the central entity which in turn broadcasts the message to each and every CR node. In Decentralized Coordinated there is no need of centralized entity in the network. In Decentralized un-coordinated method every CR node performs sensing independent of the other and leaves the band if a primary user is sensed but does not inform the other CR nodes about it.

5.3 Interference Detection:

It consists of 2 categories Interference temperature management and primary receiver detection [9]. In interference temperature management an upper bound of an interference limit is initialized for the spectrum band in a particular geographic location not permitting the CR nodes to cause hindrance using the particular band in a particular location. Its main goal is to calculate interference at the receiver. In primary receiver detection an inexpensive sensor is placed in the close vicinity of primary receiver to sense the power released by it so that it can be detected. The sensor later sends the collected data to the cognitive radio nodes to know the spectrum availability [9].

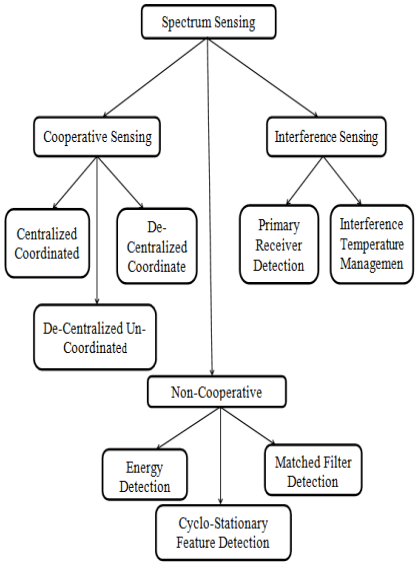

Figure 7. Spectrum Sensing Techniques

VI. SECURITY IN CRN

CRNs are flexible and unprotected as compared to conventional networks so they are more susceptible to security threats. The simplest of attack is, if the results of cognitive sensing are changed by a malicious user as a result normal functioning of the network will be disturbed. There are 3 main security needs as confidentiality, integrity and availability in CRNs [5].

6.1 Security Requisites for CRN

CRNs are more sensitive to security attacks relative to other wireless communication networks because of its inherent nature. Some of the security requisites for CRNs are as under [5]:

- ✓ Data Integrity: Data integrity is the fundamental security component in case of wireless networks as compared to networks that uses wires because WLANs are affected by burglar's users easily. Data integrity guards the

data from modification that is being transferred; there is no inserting of data or deleting of data etc.

- ✓ Data Confidentiality: Data confidentiality makes certain that the data that is being transferred is not readable to malicious users.
- ✓ Authentication: Authentication makes sure that the unlicensed users cannot approach to sensitive data. In CRNs Authentication is considered as one of the elemental security requisite for CRNs because in CRN we need to differentiate secondary users from primary users.
- ✓ Identification: Identification is defined as a procedure in which each user is given a name or identification number. In CRN each secondary user has identification method in it. Detecting the services and identifying the SUs are the fundamental components for building the adequate and authentic CRN.
- ✓ Availability: Availability is a process where authorized and non-authorized users are allowed to utilize the frequency spectrum in CRNs. In case of authorized or primary users, it means using the accessible band to transfer data and not being intervened by secondary users and in case of secondary user it means using the accessible holes of the spectrum band to transfer data and not causing any disturbance to licensed users of that band. This component helps to prohibit DoS outbreaks.
- ✓ Non-repudiation: Non repudiation prohibits the transmitter or receiver from refusing the transferred data. The non-repudiation method is useful to validate the misdeed and restrict the invader from the network if an invader is recognized as disobeying the rules.

6.2CRN Security Attacks and Defence Methods

The different security attacks on CRNs can be classified as: The physical layer attacks, the MAC layer attacks, the transport layer attacks, application layer attacks and cross layer attacks. The physical layer attacks are Primary User Emulation Attack, Objective function attack, jamming, overlapping secondary nodes. The data link layer attacks are Spectrum Sensing Data Falsification, Control Channel Saturation DoS Attack, and Selfish Channel Negotiation. The network layer attacks are HELLO flood attacks, sinkhole attacks, Sybil attack and wormhole attack. The transport layer attack is Key Depletion attack. Application layer attack includes cognitive radio viruses and cross layer attacks include lion attack and jellyfish attack.

We have two main security outbreaks the selfish attack and the malicious attacks.

- ✓ Selfish attacks: Here the mischievous user urges to utilize the band with great preference. It gives the other unauthorized users confidence that it is the authorized user of the band. Due to this the selfish user occupies the band as much as he wishes [14].
- ✓ Malicious attacks: In this the invader does not allow the other user to use the band creating the Denial of Service (DoS) [14].

- ✓ The various attacks on CRN are as follows and also shown in table 1.

6.2.1 Physical Layer Attacks:

Physical layer is the first layer of protocol stack which acts as an interface to the data communication medium. It includes everything that is required for communication between two network nodes like optical fiber, network interface card etc. and in case of CRN we can say the environment. The various attacks that target the physical layer and their defence methods are as under.

6.2.1.1 Primary User Emulation:

In PUE outbreak the mischievous unauthorized user imitates or acts as a licensed system to use the available spectrum without sharing the spectrum with other CR secondary nodes. The main motive of this attack is categorized into selfish attack and malicious attack. The PUE affects each type of radios, the policy radio and the learning radio with various austerities. In case of policy radio as early as the

intruder frees the band the aftermath of the outbreak disappears. The CR users then realize that the band is free and uses it. In case of learning radios the present and prior knowledge about licensed users is collected and the time of leaving the band is determined from it. When the spectrum is freed the intruder executes this attack and will last for a longer time. Various types of PUE attacks can take place having the little information of CRNs.

Defence Mechanisms:

For defending the PUE outbreak we need to detect the identification of the node that transmits the signals or data whether it is a licensed system or a mischievous user. However the defence methods should not make any alteration in the primary system according to FCC rules.

i. Cryptographic mechanism for authentication: e.g. digital signatures, but it has a disadvantage that it requires the modification of primary user which is not allowed by FCC protocols.
ii. Distance Ratio Test (DRT) and Distance Difference Test (DDT) [16]: DRT depends on determining the power of signal that is received and DDT depends on inequality in phases of signal. Both of them use the transmitter verification procedure. Both depends on trusted location verifiers LVs (master LVs and slave LVs). The disadvantage of DDT is that a compact synchronization is required between LVs and both of them can be deceived if the attacker is nearest to the tower.
iii. Loc-Def:InLocDef sender is verified in 3 steps: validating the signal features, analyzing the strength of received signal and localization of source. It gathers the Radio Spectrum Sensing measurements using WSN to recognize the position of sender [17].
iv. Time Difference of Arrival (TDOA) and Frequency Difference of Arrival (FDOA):It first applies TDOA and then TDOA provides some inputs to FDOA which determines the correct position of the sender [18]. It has a limitation that it is based on various hypotheses as a result it cannot be applied to CRNs.
v. Fingerprinting [19]: It authenticates the sender. Earlier RF fingerprinting was used which identifies the sender as the emitter in the waveforms. This approach is complex although it gives an optimum explanation so a new method called cross layer pattern recognition was defined to defeat this disadvantage. It uses the features of electromagnetic signatures in nodes to develop a secure system.

6.2.1.2 Objective Function Attack:

The cognitive radio is authoritative to modify various features which include frequency, bandwidth, power, modulation type, coding rate encryption type and frame size to satisfy certain criteria like less consumption of power, high data rate, and high security and each has its own weight depending on the specific operation. Cognitive radio operates on one or more features so as to reach the goal as close as possible. One or more objective functions are interpreted to achieve various features for the CR node. When cognitive radio interprets the objective function to determine the nodes features the malicious user can operate on the features which it can supervise (transfer rate) that disturbs the final results.

For example in case of emails high securityand low power may be needed while forvideos high data rate and high security maybe needed.

We consider an objective function as under[7]:

$$F=w_1P+w_2R+w_3S$$

Here w_1, w_2, w_3 are the weights associatedwith power, rate and security respectively.

For example a CR wants to use security level of s_2 but the malicious user makes it to use a lower level of s_1 i.e. $s_1<s_2$. If the user wishes to use s_2 the malicious user creates a jam in the band by reducing the R from r_2 to r_1 where $r_2>r_1$ due to which the final objective function is decreased. As a result the malicious user

enforces the CR user to implement lower security so that it can be easily breached.

Defence Mechanism: Simplest mechanism [20] is to use threshold values for the radio parameters and if the parameters do not satisfy the thresholds the interaction is halted. Its limitation is that it depends on fixed thresholds. Another method is to use good IDS. In [21, 22] the authors proposed a covert adaptive injection attack. As an example of objective function attack the malicious node is able to learn and modify its parameters according to the changing atmosphere. Here the malicious node attempts to secretly modify the sensing results of the distributed CRN, disrupting the objective function. A powerful distributed outlier detection technique is proposed to mitigate the covert adaptive injection attack. In [22] the authors used local thresholds at each device. Thus it becomes very difficult for the intruder to assume the thresholds of all the neighbouring devices at any moment. If an attacker is detected by the device it transmits a primitive alarm to its one hop neighbours. If a device receives the primitive alarms from more than half of the devices which are common neighbours of the device and the malicious device, the alarm is not dispatched rather it is broadcasted as a confirmed alarm. The attacker is validated by using hash based calculations. In [21] the authors proposed a neighbourhood voting system. Here each device after receiving the sensing data from their one hop neighbours compute algorithm based mean and performs a spatial correlation test. Every device casts a vote regarding the validity of its neighbours depending on the results. The device is declared as an attacker if more than half of neighbour's vote suspects it as the attacker.

6.2.1.3 Jamming:

In jamming the intruder can transmit data packets continuously that block the other participants of the communication to transmit or receive the data. The jammer continuously sends the data packets as a result of which the authorized user can never ever sense the channel as free or it may send the packets to the user and convince them to accept trash packets. In addition jammers are also able to disturb the interaction among users by destroying the packets in transit. More threatening effect of a jammer is that it disrupts the communication link between cognitive nodes that they use to interchange the spectrum sensing results. This type of outbreak takes place in both physical and MAC OSI layers. There are mainly 4 categories of jammers [23] as Constant Jammer which transmits the packets in continuity without waiting for the band to be free, Deceptive jammer fools the authorized users and transmits the packet towards them in continuity causing the users to shift to receiving mode, Random jammer which sends the packets in intervals i.e. it waits between the transmission of packets and at last reactive jammer which continuously watches over the band and whenever it observes interaction is taking place in the channel it sends the jamming packets. For layer 1 of OSI jamming, the intruder uses equipment that generates the energy having equal frequency used by the users to interact causing disturbance. For MAC layer jamming, the intruder transmits the packets over a specific frequency band causing other users to think that the band is busy thus, delaying their communication.

Defence Mechanism: As jamming takes place in both physical and MAC layer so it should be defended on both layers. In case of MAC layer revelation the users can determine the occurrence of outbreak by watching the band continuously using the CSMA protocol of MAC layer. In CSMA the channel is watched till it is found to be free and even after it is found free the user still waits for an arbitrary time after that it uses the channel. The CSMA will never sense the channel to be free in case the band is already in use or used by the intruder so the user backs off the communication. In case of physical layer CR nodes must be capable of detecting the abnormality in the noise level of the channels [24].

This is done by gathering the information about the noise levels in the whole network then developing a systematic model for performing the comparison when DoS attack occurs. A technique of studying the relationship between the signal strength (SS) and

packet delivery ratio (PDR) is used for jamming detection [23]. If SS is large and PDR is less the authorized user considers that jamming has occurred. This technique is called signal strength consistency checks. Other technique is the location consistency checks. Here the position of neighbours is important that can be obtained through GPS and broadcasted by every node but GPS may not always exist in CRN. The node's neighbours must have large PDR but if the neighbours have small PDR then the node is considered to be under jamming attack. Frequency hopping is a good defence technique where the participants use different channel to communicate if DoS attack takes place. Spatial retreat is a method where the participant alters its location to leave the interference range.

6.2.1.4 Overlapping Secondary Nodes:

The Dynamic Spectrum access sharing may be under threat when more than one secondary network overlap and coexist in the same geographical area either through incumbent vulnerabilities or through objective function, carried out by a malicious user or randomly by a loyal user [26][6]. Signals emitted by the malicious node in one network can affect adversely to incumbent and secondary nodes of both the networks. These emitted signals may deliver erroneous sensing data which may affect the objective function adversely in both the networks. These malicious nodes may even wrongly imitate the incumbents of both the networks periodically causing the networks to free the occupied bands. In addition to this in some cases a loyal user while declaring the appearance of incumbent in first network may recklessly deliver the similar data to the 2nd network which affects the objective function of 2nd network adversely.

Defence Method: This type of attack is difficult to mitigate because the secondary nodes of the targeted network do not have explicit control over the malicious users. This type of attack originally attacks the abilities of the CR network for performing spectrum sensing and sharing of infrastructure and Adhoc networks which is a DoS. In [25] the authors proposed three schemes for defending this type of attack which are also suitable for various other DoS attacks. The three schemes are as under:

- ✓ Modulation scheme modification [26]: The influence of DoS attacks can be reduced by using frequency hopping and direct spread spectrum methods. However they may still be able to reduce the QoS (Quality of Service).
- ✓ Detection and Avoidance of attacks [26]: A malicious user can be recognized by the network, by analyzing the incumbent's position and features of the transmitted signal.
- ✓ Adopting authentication and trust model [26]: The authors in the paper [27] developed a system to calculate certain values like trust value, suspicion level and consistency level to recognize and eliminate the malicious node. For each user trust value is determined over time while as consistency level determines the consistent trust level over time and the users become suspicious if the state of channel delivered by it does not match with the state of channel delivered by remaining users. A user will be identified as malicious and will be eliminated from the network if its trust value is consistently low.

6.2.2 MAC layer attacks:

MAC (Medium Access Control) layer is a sub-part of the data link layer which is developed to allow the medium to be shared among multiple nodes in the same network. To regulate the users access Common Control Channel is used to interchange control messages. The various attacks that target MAC layer and their defence methods are as follows:

6.2.2.1 Spectrum sensing data falsification (SSDF):

This type is also called Byzantine Attack. Here the malicious user sends the wrong sensing outcomes gathered locally either to a node or to the information gathering center due to which the node or the gathering center gives the inaccurate final verdict [28][29]. It takes place in both centralized and distributed CRNs but the attack is more dangerous for the distributed CRNs. In case of centralized, whole of the data is forwarded to the

gathering center which then decides which of the bands are free and which are busy. Tricking the center may either disallow the authorized users to utilize the band or it grants permission to the user to utilize the band that is formally busy thus effecting the communication. Same procedure is done in distributed networks but here spectrum verdicts are made co-operatively by cognitive radio nodes.

Detection and Defence Mechanism:

i. Decision fusion technique [30]: here the entire spectrum sensing result gathered locally is added up and if the addition result is > or = to a certain threshold then it determines that the band is engaged with the primary user else it is free. The limitation of Decision fusion method is that rising or reducing the threshold has great effect on the decision.

ii. Weighted sequential ratio test [31]: This test is used to defend the SSDF outbreak. It has 2 steps first is reputation maintenance step and second is the hypotheses test step. At first every node has a reputation value of 0 which is increased by 1 upon each correct sensing report. The hypotheses step depends on sequential probability ratio test.

iii. Weight based fusion scheme [32]: This is also a defending method. Here a trust approach and pre-filtering methods are used. Invaders are of 2 categories Always yes which reveals the existence of primary system and Always no that detects that the primary system is absent. It is based on pre-filtering method to detect and invalidate the intruders which are occasionally invalid and not invalid and giving every CR node a trust aspect which immediately reveals the Always yes & Always no devices.

iv. Detection Mechanism [33]: It compares the local spectrum sensing result with the global result in the fusion center over a time period. It only works when fusion center is available.

v. Bayesian detection mechanism [34]: Here former awareness about the local spectrum sensing results should be known. Its limitation is that when CRN is under SSDF attack former awareness is not authentic and thus this solution is no longer the optimal solution.

vi. Ney-man Pearson test [35]: It does not require the former awareness of final spectrum result but it requires the former awareness probabilities of local sensing. It operates by defining either the largest tolerable probability of fake alarm or largest tolerable probability of omitted detection.

6.2.2.2 Control channel saturation DoS attack:

This type of attack takes place in multi-hop CRNs. In multi-hop CRN, CR nodes interact with one another by compromising the spectrum band in a shared aspect. In this process medium access control frames are interchanged between nodes to get the spectrum band allotted to them. When more number of nodes desire to interact at the same time the CCC is saturated as it can handle only a limited number of simultaneous access to the spectrum band. The malicious user can exploit this characteristic and can produce spurious medium access control frames to saturate the band and as a result network performance decreases drastically to about zero throughput.

6.2.2.3 Selfish Channel Negotiation (SCN):

In multi-hop CRN, a CR node may refuse to send data to different devices as a result its energy is conserved and its throughput can increase because of self-centered band covering. Similarly a selfish node may modify the medium access control behaviours of the cognitive radio nodes. This attack can also decrease the throughput of the CRN drastically.

Defence method for CCSD and SCN: These attacks can be alleviated by using a trust approach allowing each cognitive radio node to be supervised and surveyed by its neighbourhood nodes. The neighbours then analyze the observed data and finally determine whether the node is mischievous or not.

6.2.3 Network layer Attacks:

Network Layer is responsible for forwarding of packets from sender device located in one network to the receiver device located on a different network.

The various problems of security in traditional wireless communications can also be found in cognitive radio networks because of the 3 shared architectures of infrastructure, Adhoc and mesh. CRNs are also similar to WSNs including multi-hop routing protocols and power constraints [26]. Frequent spectrum hand-off due to appearance of primary system makes routing more complex in CRN. The various attacks that target network layer and their defence methods are as follows:

6.2.3.1 Sinkhole Attacks [36]:

Sinkhole attacker deceives other nodes that it is the perfect path towards a particular destination thus inviting them to forward the packets through it. Here the intruder is also able to alter or drop the packets from various devices within the network such process is known as selective forwarding. This type of outbreak is more powerful in mesh and infrastructure architectures as all the packets first travel to the base station which permits the intruder to dictate that it is the most appropriate path for passing the packets through the network.

Defence Methods: This type of attack is difficult to detect. Geographic routing [36] protocols develop a topology on demand using only interactions done locally and data without the help of base station. As a result data will be passed to the base station and will not go anywhere else to produce a sinkhole.

6.2.3.2 Hello flood Attacks [36]:

Here the intruder broadcasts the message to all the CR nodes of the network with sufficient power that it is in the neighbourhood of them. For instance the intruder may send the packet to the nodes informing them that it is their neighbour and should be used for transmitting the packets to the specific nodes as a result even the far off nodes will use this node for transmitting their packets to specific destination. But these packets may be lost, also if the node suspects the outbreak it cannot send the packets because other nodes may also use the same intruder node to transfer the packets.

Defence: To alleviate this attack a symmetric key is shared between a node and the base station behaving as a trusted third party and establishes the session keys between the participating entities to secure their communication. The 2 parties use the session keys to identify one another and authenticate also.

6.2.3.3 Sybil Attack: Sybil attack is a type of attack where the attacker produces a huge number of fictitious identities and acts like geographically different devices [37]. As it is a complex task to keep a database of different identities because of the existence of many small scale networks managed by multiple managers, CRNs are susceptible to these type of attacks. In the CR network where many devices are striving for white bands, a malicious device may produce a number of fictitious identities. Each of the fictitious identity makes a request for the frequency band as a result fairness of spectrum usage is reduced for other legitimate devices [38].

Defence Methods: The main idea for defending the Sybil attack is to validate each devices identity.

Usually there are two methods to validate the identity as direct and indirect validation. In case of direct validation, validation of one device is checked directly by other device and in case of indirect validation devices that are already validated, validate the identity of other devices. In [37] a method resource testing is proposed for direct validation. Resource testing is based on the assumption that the resources of malicious node's physical entity are limited. The device is validated by measuring the resources and comparing them with the resources of physical node. In [39] proposed a different validation technique for CRNs, the radio resource testing channel. The various assumptions for this technique are: Firstly each physical device consists of only one radio and secondly each radio can only transmit or receive data over one channel at any instant. A device then verifies that its neighbouring devices are not Sybil attackers by allocating a distinct channel to each and every neighbouring devices on which they can broadcast the packets. A channel is then selected randomly by the challenger on which it listens to the

packets to determine whether the neighbour to which channel is assigned is an authentic one or not. The main limitation of Radio resource testing method is that if there is not sufficient number of channels to allocate each neighbour with a different channel.

6.2.3.3 Wormhole Attack:

In wormhole attack, the malicious node receives the packets in one portion of the network and dispatches them over wired or wireless communication link with lower latency than the default ones. The packets are replayed in other portion of the network. This type of attack is carried out by the authentic users mostly few hops away from base-station that they are only one or two hops far through the attacker [26]. Mostly the users in the network may use the adversary for dispatching of messages when the edge of the wormhole is far away from the base-station. As a result messages may be transmitted selectively to the adversary device that are nearer to base-station for additional dispatching or collected for snooping as they are forwarded [26]. The wormhole attack may result in the division of the network if the attackers are correctly placed. This division of network leads to network route discovery which gives extra knowledge to the attackers to be utilized for different types of attacks [26].

Defence Methods: In [36] proposed to utilize geographic routing protocols to transmit messages within the network. These geographic protocols build a network topology on routing the messages to the base-station which makes it difficult to divert messages to the wormhole. In [40] the authors suggested adopting packet leashes to reveal and mitigate this type of attack. The paper proposed two different types of packet leashes that is geographic and temporal which ensures that the attacker is detected if the packet is moved more than the allowed leashes. Geographic leash makes sure that the destination of the packet is not so far from the transmitter. For this type of leash every device should have the knowledge of their own position and their clocks should also be roughly synchronized.

The transmitter appends their position to the packet and the instant the packet was transmitted. The destination device correlates this information with its position and the time instant of receiving the packet. The destination device calculates the upper bound of the radius among the transmitter and itself. On the other hand temporal leash maintains an upper bound on the duration of packet life which limits the longest navigation length of the packet. In temporal leash the clocks should be tightly synchronized. The transmitter appends the instant when the packet was transmitted, to the packet. The destination correlates the time when the packet was received to the time when it was transmitted due to which the destination gets to know whether the packet had travelled too far or not.

6.2.4 Transport layer Attack:

The transport layer is responsible for flow control, error control and congestion control. The attack that targets transport layer and its defence method is as under:

6.2.4.1 Key Depletion Attack:

The TCP session times in CRN are shorter because of the large round-trip-time and too many retransmissions [41]. This implies that a large number of TCP sessions are initiated. At the start, each TCP session is associated with a cryptographic key in various transport layer protocols like SSL. As more and more session keys are used there is a chance that some keys may be duplicated. This duplication of keys can be exploited by the attacker to breach the basic cipher system [26]. Various protocols like wired equivalent privacy (WEP) protocol and temporal key integrity protocol of IEEE 802.11 are vulnerable to key repetition attacks [26].

Defence Method: CCMP (counter cipher mode with block chaining message authentication code protocol) is developed to exponentially deplete key

duplications [29]. The proposed protocol uses 128 bit keys associated with 48 bit initialization vector. This approach decreases the susceptibility of the network to replay attacks [26].

6.2.5 Application Layer Attacks:

Application layer is the last layer of protocol stack and is the nearest to the final user. This layer has the authority to compute the resources that are available, to synchronize the data transmission and recognizing the nodes. Due to additional responsibility of spectrum sensing and learning, Cognitive Radios need larger transmitting power as compared to classical radios. So they are vulnerable to software viruses and malware [26]. Also, the delays that occur at physical and MAC layer because of frequent handoffs, irrelevant re-forwarding of packets and those that occur due to numerous key exchanges results in decrease in quality of service at application layer [26].

6.2.5.1 Cognitive Radio Virus [26]:

Virus is a malicious program that duplicates itself when executed or poisons other programs by making alterations in them. CRNs are susceptible to viruses in the same manner as the other networks. In CRNs these viruses can be destructive because of its self -propagating nature. A cognitive radio affected by the virus can propagate to other neighbouring radios an invalid state. The neighbour radio will pass through this invalid state and the radio will falsely learn to adapt to this atmosphere thus influencing the decision of the network.

Defence Method: In [7] the authors introduced a feedback loop into the network that enables the cognitive radio to perform learning again when invalid information about the environment is propagated. Another technique is to develop method to disqualify learned actions that are expected to defy certain rules.

6.2.6 Cross layer Attacks:

Cross-layer attacks are those attacks that target more than one layer of protocol stack which can disrupt the entire cognitive process of spectrum sensing, analysis and decision [26]. Here the attacker may target one layer however the performance of other layer may be degraded. Various cross layer attacks are as follows:

6.2.6.1 Lion Attack [42]: This attack uses the primary user emulation attack to disturb the TCP links. It is a cross layer attack executed at the physical layer and intended at transport layer where masking an authorized transmission forces a cognitive network to execute frequency hopping and thus transmission control protocol performance will be degraded. Whenever the PUE outbreak occurs all unauthorized users of the band will perform frequency handoffs but TCP will not be aware of these handoffs so it will continue to create logical connections and sending packets with no confirmation from the receiver. When the time of TCP segments will be over then TCP will retransmit the packets with large timeout. As a result there will be more delay and packets will be lost.

Defence Method: To defend this attack a method [43] is used in which transport layer is made conscious about the happenings at the physical layer by sharing of data between physical and transport layer. Due to this, the TCP connections will be stopped during the frequency hand off periods and later readjust them according to the newer network circumstances. Cross Layer Detection, based mechanism is used to detect the attack. It is a good solution.

6.2.6.2 Jelly-Fish Attack: It is similar to lion attack because both affect the TCP [26]. In case of lion attack deterioration of TCP occurs because of frequent spectrum handoff. While in case of Jellyfish attack the reduction in throughput takes place due to

packets arrived out of order, delayed or dropped [26]. It is executed at the network layer and targets the transport layer. The packets received are deliberately rearranged by the attacker. TCP is susceptible to out of order packets because they provoke retransmissions and deteriorate throughput. Dropping of packets can also deteriorate throughput [26].

Defence Methods: In [44] the authors presented a mitigation method in which each device examines their neighbour's movements. The devices calculate the ratio of dropped packets in a certain time span for its neighbours that drop packets. This ratio is compared with predefined threshold and if it is more than the threshold, then its neighbours that are at one hop distance to the device dismiss it for a certain time span. In [45] a method is proposed that uses the broadcast nature of wireless medium for detection and mitigation of these attacks. Here the attack can be detected by its neighbours when they are set to examine the activities of one another. In this method packet are transmitted with cumulative sequence numbers and ID number. The nodes that are examining the activities of other nodes are able to detect delayed, dropped or out of order packets if any, by its neighbour. If a threshold of this malicious behaviour is exceeded the malicious node is penalized and can even be thrown out of the network.

Table 1. Table Of Various Types Of Attacks On Different Layers

S.No.	Type Of Attack	Layer	Corrective Measure	Assessment
1.	PUE	Physical Layer	• Cryptographic method • DRT-depending on SS measures • DDT- depending on signal phase difference • LocDef- depending on location of transmitters • TDOA & FDOA • Fingerprinting	• It violates FCC rules as it involves modification of primary system • Main limitation is the compact synchronization is needed between LVs and can be tricked if intruder is in the vicinity of the transmitter • Same as DRT • Main limitation is the incorporation of WSN • The main limitation is that it depends on various assumptions as a result they cannot be used in CRNs • This is the good mechanism
2.	Objective Function attack	Physical layer	• Assign a threshold value to each and every CR parameter if the parameter does not satisfy the threshold value then interaction halts • Using IDS	• The main limitation of this is that it needs to define thresholds which are static. • IDS cannot be used to oppose all types of outbreaks • It is a good method but requiresto define thresholds • It is a good method

			• Method based on local thresholds • Neighborhood voting system	
3.	Jamming	Physical layer	• Create a statistical framework to define the difference among natural and unnatural levels of noise • Comparison between SS and PDR- if SS is large and PDR is small the node is blocked if one of the neighboring nodes do not have large SS and PDR • Location Consistency checks • Frequency Hopping • Spatial method	• Limitation is the amount of information needed to create a statistical framework. • This is a weak approach as there is no relation in large and small • The limitation is that a GPS is required but it may not be always available • This is an appropriate method • Here the CR node must be attentive when it leaves the area of intruder as it still needs to remain within the area of reach to other nodes it is interacting.
4.	Overlapping Secondary Nodes	Physical layer	• Modulation scheme modification • Detection and Avoidance of attacks • Adopting authentication and trust model	• All three are good defence methods
5.	SSDF	MAC layer	• Fusion method in which entire sensing results are added up and then related to threshold to disclose the outbreak. • Weighted sequential ratio test • Weight based fusion method • Method that need previous information • Neyman-Pearson Test	• Here raising or reducing the threshold is the main limitation. • This is good method • This is also good method • Limitation is when the network is under SSDF outbreak the previous probability information may not be truthful. • It also need previous probability information
6.	CCSD	MAC layer	• Trust based method	• This is a good method

7.	SCN	MAC layer	• Trust based method	• This is good approach
8.	Sinkhole	Network layer	• Protocols based on geographic routing	• This is a good approach
9.	HELLO flood	Network layer	• Algorithm based on symmetric key	• This is a good approach
10.	Sybil Attack	Network layer	• Radio resource Testing Method • Resource testing •	• The main limitation of Radio resource testing method is that if there is not sufficient number of channels to allocate each neighbor with a different channel. • It is a good technique
11.	Wormhole Attack	Network Layer	• Utilization of Geographic Routing Protocols • Packet Leashes: Geographic and temporal	• It is a good technique • Geographic leashes are less efficient than temporal as they require broadcast authentication, but can be used in networks where precise time synchronization is not easily achievable
12.	Key Depletion	Transport layer	• Counter Cipher mode with block chaining message authentication code protocol (CCMP)	• It is a good technique
13.	Cognitive Radio Viruses	Application Layer	• Inserting a feedback loop into the network	• It is a good technique
14.	Loin Attack	Cross layer	• Cross layer detection method	• This is a good approach
15.	Jellyfish Attack	Cross layer	• A mitigation method in which each device examines their neighbour's movements. • A method that uses the broadcast nature of wireless medium for detection and mitigation of these attacks.	• Both techniques need to define the thresholds

VII. CONCLUSION

Cognitive Radio Network is an encouraging technology for productive use of spectrum and also allows flexible communication anytime and anywhere. CRN is vulnerable to various types of attacks in spite of its promising applications. In this paper we have intensively studied about CRN, its

working process and architecture, various attacks and defence methods in various layers. Current security research in CRN has mainly concentrated on the attacks like spectrum sensing data falsification, jamming and primary user emulation. Additional research needs to be done for secure transport protocols for CRNs, viewing the networks exclusive features in spectrum management and spectrum mobility and also in the area of cognitive radio Adhoc networks handling their different security problems. Also research needs to be done to defend the CRN functions from various classical risks like viruses, Trojans etc. as well as advanced risks that affect the cognitive radios learning capability. Even though various defence methods for different attacks have been proposed but there is a need to provide a generalized defence method for Cognitive Radio Networks eliminating the need to employ protection mechanism at each and every layer.

VIII. REFERENCES

[1]. Beibei Wang and K. J. Ray Liu, "Advances in Cognitive Radio Networks: A Survey," IEEE Journal of Selected Topics in Signal Processing, vol. 5, no. 1, (Wang & Liu) February 2011.

[2]. Wassi (Wang & Liu, 2011)m El-Hajj1, Haidar Safa1, Mohsen Guizani, "Survey of Security Issues in Cognitive Radio Networks," Journal of Internet Technology Volume 12 ,2011.

[3]. Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran , Shantidev Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," Computer Networks. Elsevier, 2006.

[4]. F.K. Jondral, "Software-defined radio-basic and evolution to cognitive radio," EURASIP Journal on Wireless Communication and Networking 2005.

[5]. Sazia Parvin , FarookhKhadeerHussain , OmarKhadeerHussain , SongHan , BimingTian , Elizabeth Chang, "Cognitive radio network security: A survey,"Elsevier Journal Of Networks and Computer Applications 35, 2012.

[6]. Yenumula B. Reddy, " Security Issues and Threats in Cognitive Radio Networks," AICT 2013:The Ninth Advanced International Conference on Telecommunications.

[7]. T. Charles Clancy, Nathan Goergen, "Security in cognitive radio networks: threats and mitigation," 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008. Crown Com 2008, 2008, pp 1–8 (IEEE).

[8]. J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Ph.D. Dissertation, KTH, 2000.

[9]. Mansi Subhedar1 and Gajanan Birajdarok, "Spectrum Sensing Techniques in Cognitive Radio Networks: a survey," International Journal of Next-Generation Networks (IJNGN) vol.3, no.2, june 2011.

[10]. Ekram Hossain, Vijay Bhargava (2007), "Cognitive Wireless Communication Networks", Springer

[11]. D. Cabric, A. Tkachenko, and R. Brodersen, (2006) "Spectrum sensing measurements of pilot, energy and collaborative detection," Proceeding of IEEE Military Commun. Conf., Washington,D.C., USA, pp: 1-7.

[12]. Ian F. Akyildiz, Brandon F. Lo, Ravikumar (2011), "Cooperative spectrum sensing in cognitiveradio networks: A survey, Physical Communication", pp: 40-62.

[13]. A. Min, K. Shin, (2009), "An optimal sensing framework based on spatial RSS profile in cognitive radio networks", Proceedings of IEEE SECON, pp: 1-9.

[14]. Rajesh K. Sharmaand Danda B. Rawat, "Advances on Security Threats and Countermeasuresfor Cognitive Radio Networks: A Survey" IEEE Communications Surveys & Tutorials.

[15]. Gaurav Bansal, Md. Jahangir Hossain, Praveen Kaligineedi, Hugues Mercier, Chris Nicola, Umesh Phuyal, Md.Mamunur Rashid, Kapila C. Wavegedara, Ziaul Hasan, Majid Khabbazian,

and Vijay K. Bhargava, "Some Research Issues in Cognitive Radio Networks,"IEEE 2007.

[16]. Ruiliang Chen and Jung-Min Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," First IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), Reston, VA, September, 2006, pp.110-119.

[17]. Ruiliang Chen, Jung-Min Park and Jeffrey H. Reed, "Defence against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE Journal on Selected Areas in Communications, Vol.26, No.1, 2008, pp.25-37.

[18]. Lianfen Huang, Liang Xie, Han Yu, Wumei Wang and Yan Yao, "Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks," International Conference on Communications and Mobile Computing (CMC), Vol.2, Shenzhen, China, April, 2010, pp.169-173

[19]. O. Richard Afolabi, Kiseon Kim and Aftab Ahmad, "On Secure Spectrum Sensing in Cognitive Radio Networks Using Emitters Electromagnetic Signature," Proceedings of 18th International Conference on Computer Communications and Networks (ICCCN 2009), San Francisco, CA, August, 2009, pp.1-5.

[20]. Olga León, Juan Hernández-Serrano and Miguel Soriano, "Securing Cognitive Radio Networks," International Journal of Communication Systems, Vol.23, No.5, 2010, pp.633-652.

[21]. Changlong Chen, Min Song, Chunsheng Xin, Mansoor Alam, "A robust malicious user detection scheme in cooperative spectrum sensing,"Global Communications Conference (GLOBECOM),2012 IEEE, pp. 4856–4861.

[22]. Qiben Yan, Ming Li, Tingting Jiang, Wenjing Lou, Y. Thomas Hou, "Vulnerability and protection for distributed consensus based spectrum sensing in cognitive radio networks,"2012 Proceedings IEEE INFOCOM, 2012, pp. 900–908 (IEEE).

[23]. Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, "The Feasibility of Launchingand Detecting Jamming Attacks in Wireless Networks," Proceedings of ACM MobiHoc, Urbana, IL, May, 2005, pp.46-57.

[24]. Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, "Channel Surfng and Spatial Retreats: Defences Against Wireless Denial of Service," Proceedings of the 3rd ACM Workshop on Wireless Security, Philadelphia, PA, January, 2004, pp.80-89.

[25]. Saman T. Zargar, Martin B.H, Weiss, Carlos E. Caicedo, James B.D. Joshi, "Security in Dynamic Spectrum Access Systems: A Survey," University of Pittsburgh, 2011, <http://d-scholarship.pitt.edu/2823/>.

[26]. Deanna Hlavacek, J. Morris Chang, "A layered approach to cognitive radio network security: A survey,"Computer Networks 75 (2014) 414–436, Elsevier.

[27]. Wenkai Wang, Husheng Li, Yan Sun, Zhu Han, "Attack proof collaborative spectrum sensing in cognitive radio networks," 43rd Annual Conference on Information Sciences and Systems,CISS 2009, pp. 130–134 (IEEE).

[28]. Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Berkeley, CA, May, 2003, pp.113-127.

[29]. Chetan Mathur and Koduvayur Subbalakshmi, "Security Issues in Cognitive Radio Networks," Cognitive Networks: Towards Self-Aware Networks, Wiley, New York, 2007, pp.284-293.

[30]. A. Pandharipande et al., "IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22," IEEE 802.22 WG on WRANs, November, 2005

[31]. Ruiliang Chen, Jung-Min Park, Y. Thomas Hou and Jeffrey H. Reed, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE Communications Magazine, Vol.46, No.4, 2008, pp.50-55.

[32]. Praveen Kaligineedi, Majid Khabbazian and Vijay K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," IEEE International Conference on Communications 2008 (ICC '08), Beijing, China, May, 2008, pp.3406-3410.

[33]. Ankit Rawat, Priyank Anand, Hao Chen and Pramod Varshney, "Countering Byzantine Attacks in Cognitive Radio Networks, 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)," Dallas, TX, March, 2010, pp.3098-3101.

[34]. Linjun Lu, Soo-Young Chang et al., "Technology Proposal Clarifications for IEEE 802.22 WRAN Systems," IEEE 802.22 WG on WRANs, March, 2006.

[35]. Joerg Hillenbrand, Timo Weiss and Friedrich K. Jondral, "Calculation of Detection and False Alarm Probabilities in Spectrum Pooling Systems," IEEE Communication Letters, Vol.9, No.4, 2005, pp.349-351.

[36]. Chris Karlof and David Wagner, "Secure Routing in Wireless Networks: Attacks and Countermeasures," Ad Hoc Networks, Vol.1, 2003, pp.293-315.

[37]. J.R. Douceur, "The Sybil attack," Proceedings of 1st International Workshop on Peer to Peer Systems (IPTPS), Springer, 2002.

[38]. Shameek Bhattacharjee, Shamik Sengupta, Mainak Chatterjee, "Vulnerabilities in cognitive radio networks: A survey" Computer Communications 36 (2013) 1387–1398, Elsevier.

[39]. James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, "The Sybil attack in sensor networks: analysis & defences," Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, 2004, pp. 259–268 (ACM).

[40]. Y.C. Hu, Adrian Perrig, and David B. Johnson, "Packet leashes: a defence against wormhole attacks in wireless networks," INFOCOM 2003. Twenty-Second Annual Joint Conferenceof the IEEE Computer and Communications, IEEE Societies, vol. 3, 2003, pp. 1976-1986 (IEEE).

[41]. H.M. Qusay, D. MAHMOU, "Cognitive Networks: Towards Self-Aware Networks," Wiley, London, 2007.

[42]. Olga León, Juan Hernandez-Serrano and Miguel Soriano, "A New Cross-Layer Attack to TCP in Cognitive Radio Networks," Proceedings of the 2nd International Workshop on Cross Layer Design (IWCLD '09), Palma, Spain, June, 2009, pp.1-5.

[43]. Juan Hernandez-Serrano, Olga León and Miguel Soriano, "Modeling the Lion Attack in Cognitive Radio Networks," EURASIP Journal on Wireless Communications and Networking, Vol.2011, Article ID 242304, 10 pages, 2011.

[44]. Ning Jiang, Kien A. Hua, Danzhou Liu, "A scalable and robust approach to collaboration enforcement in mobile ad hoc networks," J. Communication Networks 9 (1) (2007) 56.

[45]. Fahad Samad, "Securing Wireless Mesh Networks: A Three Dimensional Perspective," PhD thesis, University bibliothek, 2011.