*ACCENTS Transactions on Information Security, Vol 1(1)*
*ISSN (Online): 2455-7196*

**Review Article**

# Security issues and challenges in cognitive radio network : a comprehensive study

**Kaustav Ghosh***
Department of Computer Science (MCMS) St. Xaviers College Autonomous (Kolkata) , India



## Abstract
***In the present paper the author will discuss the cognitive radio network (CRN) architectures as well as the various layers of CRN. The author will focus on security issues in CRN. As CRNs are a special kind of Ad Hoc network only, most of the attacks subjected to Ad Hoc networks can also target CRNs. The work analyzes the various attacks that are most relevant to CRNs and ways to defend against them.***

## Keywords
***Base station, access point, MAC-sub-layer, Denial of service, Fusion center, Throughput, cross-layer, Digital signature, FCC, Distance ratio Test, Distance difference test, CSMA, Packet delivery ratio, Trust value indicator, Kerberos, Group key management.***

## 1.Introduction
Intellectual Radio is a radio for remote interchanges in which either a system or a remote hub changes its transmission or gathering parameters taking into account the cooperation with the earth to convey effectively without interfering with the licensed users, serving the secondary users in an intelligent way [4]. In today's world wireless communications are used in almost every field ranging from personal sphere where cell phones and televisions are abundant to commercial spheres where Near Field Communication is the latest technology holding personal information aiding communication for commercial use. Governmental capacities also use wireless communication to spread awareness about natural disasters or national movement of any kind. All these adds up to overcrowding of certain spectrums, even creating bottlenecks at certain situations while leaving some under-utilized. Thus efficient spectrum utilization is a major problem requiring immediate look after. In countries governmental organizations and standards bodies like International Telecommunication Union (ITU) and European Telecommunications Standards Institute (ETSI) are involved in the spectrum management process known as spectrum allocation. This makes the problem of efficient spectrum utilization even more drastic.

The proposal of cognitive radio provides an innovative and much awaited solution to improve spectrum utilization efficiency. It has technology enabled for dynamic spectrum access as well as ability to adjust to use vacant spaces in an intelligent way, learning from its previous transmissions.

## 2.Cognitive radio networks architecture
The equations are an exception to the prescribed specifications of this template. You should figure out if or not your mathematical statement ought to be written utilizing either the times new roman or the image textual style (satisfy no other text style). To make multileveled comparisons, it might be important to regard the mathematical statement as a graphic and insert it into the text after your paper is styled. The authors of [1] organized CRNs into three different architectures namely Infrastructure architecture, Ad-Hoc architecture and Mesh architecture.

### 2.1Infrastructure architecture
An infrastructure CRN consists of a **base stations** or **access points** which are devices having CR capabilities. The base stations communicate with other devices within its respective range through the base station itself. Communication between devices in cells other than itself is routed by the base stations.

### 2.2Ad Hoc architecture

*Author for correspondence

Ad-hoc CRNs consists of devices that do not need base stations, the devices can establish links between each other using different communication protocols. Existing protocols like Bluetooth may be used by them. The use of spectrum holes is also quite prevalent among them.

### 2.3Mesh architecture

Mesh architecture can be considered as a combination of infrastructure architecture and ad hoc architecture. In mesh architecture devices connect to the base stations through neighboring devices with the base stations working as routers forwarding packets.

## 3.Layers of cognitive radio network [3]

The Cognitive radio Network contains the following layers:

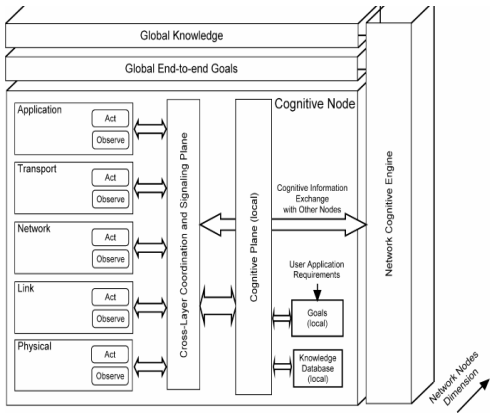


**Figure 1** Layered architecture of cognitive radio

### 3.1Physical layer

The primary function of the physical layer of a cognitive radio is spectrum sensing. Physical layer looks after the interaction between data link layer and physical wireless medium. Cognitive radio considers the situations where both primary and secondary users occupy the same channel space like in case of licensed band scenarios. Physical layer also does the work of reconfiguration of the transmission parameters for a cognitive radio prior to its transmission in the detected spectrum. As a matter of fact the main difference between the physical layer of a cognitive radio network and the physical layer of other wireless networks is that Cognitive Radio is capable of reconfiguring its operating frequency, modulation, channel coding and output power based on generic hardware.

### 3.2Data link layer

The primary function of cognitive radio networks' data-link layer is spectrum sharing. Data Link layer is known for spectrum sharing because issues related to a radio's access to spectrum are typically concerned with MAC sub-layer. Basic difference between generic MAC and MAC for cognitive radios is that coexistence between licensed and unlicensed users, dynamic selection of a frequency to transmit in a range of available spectrum and transmitter-receiver handshakes where two or more cognitive radios must agree on a mutual channel upon which to communicate. Generally, efficient medium access control (MAC), and error control and correction are the main function of link layer (The link layer is the lowest layer in the Internet Protocol Suite, commonly known as TCP/IP, the networking architecture of the Internet. The link layer is often described as a combination of the data link layer and the physical layer in the OSI model).

### 3.3Network layer

Cognitive radio networks unlike traditional self-organizing wireless ad hoc networks do not work with a single fixed frequency band. Cognitive radios can opportunistically utilize various spectral holes, white spaces, for peer-to-peer communications. Cognitive network protocols support variety of higher layer applications like voice, data, video, and mobile real-time services, as traditional wireless networks. Moreover they have to be aware of rapidly changing radio environment, access to multiple radio channels, and physical layer and MAC dedicated spectrum usage.

### 3.4Transport layer

Transport layer primarily concentrates on end-to-end reliable delivery of event readings and dealing with congestion control. When an event is detected, sensor nodes feed high and busty traffic into the network, to achieve successful detection and tracking of an event signal. Adequate number of event readings has to be reliably delivered to the receiver end. In case the capacity of multi-hop network exceeds at that time it would lead to congestion which wastes power and communication resources of network. Thus there is a relation between reliability and energy-efficiency, which has been the main focus for proposed transport layer for cognitive sensor networks. None of the available transport layer solutions for traditional wireless network, which guarantees reliable delivery with minimum energy consumption and congestion avoidance, can be considered for dynamic spectrum

access, so there exists no transport layer solution for ad hoc cognitive radio networks too.

### 3.5Application layer

Application layer provide methods to query sensors, interest and data circulation, data aggregation and fusion. No application-layer protocol have been developed specifically for Cognitive Radio Network as yet. As per the authors of [3] the application layer algorithms mainly deal with the generation of information and extracting the features of event signal being monitored to be communicated to the receiver end In wireless networks, the layered architecture of protocol design cannot provide optimal performance. To achieve high end-to-end throughput, to increase the network capacity and utilization and to reduce interference and power consumption for various applications the authors of [5] proposed a cross-layer design.

The cross- layer design can be done between physical and data link layers, data link and network layer, network and transport layer, data link and transport layer etc.

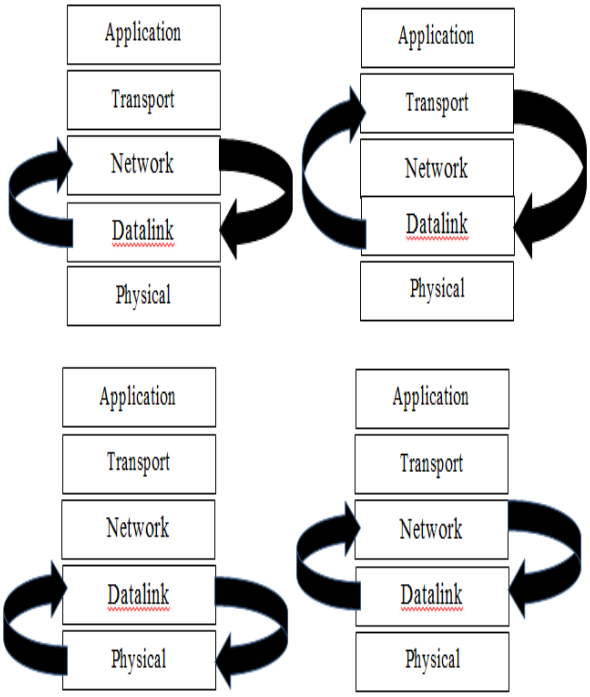


**Figure 2** Various cross layer designs

In cognitive radio networks, the cognitive engine at the heart of cognitive radio will leverage on cross-layer information exchange and inter- actions with different wireless interfaces and devices in order to achieve the best quality of service for all communications.

## 4.Attacks on Cognitive Radio Networks

The attacks on cognitive radio networks can be categorized according to the layers they target: Physical layer, Data Link layer, Network layer, and Transport layer.

### 4.1Physical layer attacks

#### 4.1.1Primary user emulation

[1] [2] According to the principle of Cognitive Radio a secondary user is allowed to use a specific band as long as it's not occupied by a primary user. If the secondary user detects the presence of a primary user, it must switch channels immediately to an alternative band in order not to cause interference to the primary user. If it happens that a secondary user detects another secondary user using the same band, the spectrum must be shared fairly using certain mechanisms.

Primary User Emulation (PUE) attack is carried out by a malicious secondary user masquerading as a primary user to obtain the resources of a given channel without having to share them with other secondary users. In doing so the attacker obtains full bands of a spectrum.

The purpose behind the attack is divided into two categories:

**Selfish PUE attack:** In the Selfish PUE attack, the attacker aims to increase its share of spectrum resources. Selfish PUE can be conducted simultaneously by two attackers to establish a dedicated link between them.

**Malicious PUE attack:** In the Malicious PUE attack, the attacker tries to prevent legitimate secondary users from using the spectrum holes.

#### 4.1.2Objective function attack

[1] [2] Cognitive radios sense the environment, learn from the history, and make intelligent decisions to adjust their transmission parameters according to the current state of the environment. The intellectual motor in the versatile radio is the one in charge of modifying the radio parameters keeping in mind the end goal to meet particular necessities, for example, low vitality utilization, high information rate, and high security. Radio parameters are for example center frequency, power, bandwidth, modulation type, coding rate, channel access protocol, encryption type and frame size.

The cognitive engine calculates the abovementioned parameters by solving objective functions like finding the radio parameters maximizing data rate and minimizing power. When the cognitive engine is running to find the radio parameters appropriate to the current environment, the assailant can dispatch his assault by controlling the parameters he has control on like transmission rate in order to make the results best suited to his interest.

#### 4.1.3Jamming

[1] [2] In jamming, the attacker known as a jammer maliciously sends out packets to obstruct legitimate participants in a communication session from sending or receiving data; consequently, creating a denial of service situation. The jammer may send continuous packets of data making a legitimate user to never sense a channel as idle, or he can send these packets to the legitimate users and force them to receive junk packets. The jammer can damage a communication by blasting a radio transmission too, resulting in the corruption of packets received by legitimate users.

The most dangerous of all attacks a jammer can do is to jam the dedicated channel that is used to exchange sensing information between CRs. Jamming is an attack that can be done in the physical and MAC (one of the two sub layers of the data link layer) layers. There exist four sorts of jammers: Constant Jammer, Deceptive Jammer, Random Jammer, and Reactive Jammer.

### 4.2Link layer attacks

#### 4.2.1Spectrum Sensing and Data Falsification (SSDF) Attack

**[1] [2]** Spectrum Sensing Data Falsification, also known as the **Byzantine Attack**, takes place when an attacker sends **false local spectrum sensing results** to its neighbors or to the **fusion center**, causing the receiver to make a wrong spectrum-sensing decision. SSDF targets **centralized CRNs** as well as **distributed CRNs**. In the centralized CRN fooling the fusion center will either deny some legitimate users from using a free band or allow users to use a band that is already occupied causing interference. Similar problems occur in a distributed CRN as well. SSDF attack may well prove to be more harmful in a distributed CRN as the false information may propagate rapidly with no ways to control them.

#### 4.2.2Control channel saturation denial of service attack (CCSD)

[1] [2] In a multi-hop CRN, Cognitive radio set communicate with each other after acting a channel negotiation process in a distributed manner. In the negotiation phase, MAC control frames are exchanged to engage the channel. Often when many CRs want to communicate at the same time, the common control channel becomes a bottleneck as the channel can only support a certain number of concurrent data channels. An attacker can utilize this feature and generate false MAC control frames thus saturating the control channel and decreasing the network performance due to Link layer collisions.

The Control Channel Saturation Denial of Service Attack leaves the CRN with a near-zero throughput. CCSD attack works only on multi- hop CRNs and does not work on centralized CRN.

#### 4.2.3Selfish channel negotiation (SCN)

[1] [2] In a multi-hop CRN, a CR host can spurn to forward any data for other hosts. This will allow it to conserve its energy and increase its own throughput which resulted from selfish channel concealment. Similar object can be achieved if the selfish host was able to alter the proper Medium Access Control behavior of the cognitive radio set devices. For instance, if the host decreases its own back-off window size, it will have a higher chance of claiming the channel at the expense of other CR hosts. SCN can severely degrade the end-to-end throughput of the whole CRN.

### 4.3Network layer attacks

#### 4.3.1 Sinkhole attack

[1] [2] In a sinkhole attack, an attacker announces itself as the best route to a particular destination, luring neighboring nodes to use it to forward their packets. An assailant might utilize along these lines to perform another assault called particular sending where an attacker is able to modify or discard packets from any node in the network.

#### 4.3.2HELLO flood attack

[1] [2] In the HELLO flood attack the attacker sends a broadcast message to every one of the hubs in a system with enough energy to persuade them that it is their neighbor. An attacker sending a packet announcing a high quality link to a specific destination will encourage even far away nodes to use this route getting convinced that he is their neighbor.

### 4.4Transport layer attacks

#### 4.4.1.Lion attack

[1] [2] The Lion attack uses the PUE attack to unsettle the Transmission Control Protocol connection. The Lion attack in a sense can be considered a cross-layer attack as well. It is performed at the physical link layer and targeted at the transport layer where imitating an authorized

transmission will constrain a CRN to perform recurrence handoffs and subsequently deteriorating TCP performance. During a PUE attack all secondary users do frequency handoff in order to free the channel for the primary user. When this handoff takes place, TCP remains unaware of the handoff and continues to create logical connections and sends packets without receiving any acknowledgment. The TCP segments then start to get timed out and in turn TCP retransmits them with an increased timeout value. Subsequently, the retransmission clock backs off multiplying the quality, bringing about deferrals and packet loss. At this point if an attacker can intercept the messages, it can predict the frequency band tested in a handoff, and claim it using PUE resulting in a total network starvation.

## 5. Defending against cognitive radio network attacks

### 5.1Defending against primary user emulation attack

[1] To protect against PUE assaults the personality of the transmitting source should be recognized, i.e., whether the transmitting source is an essential client or a malignant client? The usual as well as the best approach of knowing whether the user is a primary user or a malicious user is to apply cryptographic authentication mechanisms like digital signatures. But such an approach cannot be adapted because of the FCC (Federal Communications Commission) regulation that prohibits altering primary user systems. Given this restriction and knowing that primary users' locations are known ahead of time it was resorted to finding efficient ways of pin pointing the location of the transmitting source.

According to the author of [1] if the location of the source matches with the location of a primary user, the source is considered to be a primary user else it is considered to be an attacker trying to imitate ("emulate") a primary user. Two approaches have been suggested by the same to determine the location of the transmitting source:

Distance Ratio Test (DRT): Based on received signal strength measurements Distance Difference Test (DDT): Based on signal phase difference.

Both DRT and DDT are based on a transmitter verification procedure. The procedure makes use of a location verification method to differentiate between primary signals and secondary signals masquerading as primary signals. Certain assumptions are made regarding the environment where the attack is likely to occur.

### 5.2Defending against objective function attack

[1] No good solution has been suggested as yet to defend the Objective Function Attack. A simple suggestion may be to define threshold values for every updatable radio parameter. If the parameters do not meet the thresholds, the communication stops.

Intrusion Detection System (IDS) can also be used to defend against Objective function attack.

### 5.3Defending against jamming

[1] As Denial of Service can be performed at the link layer as well as the physical layer, the detection of denial of service should be addressed at both layers.
In the MAC-layer (a sub-layer of the data link layer) detection, devices can detect a denial of service attack by sensing the channel they want to transmit their packets on. This can be done using CSMA protocol. In CSMA, a device will continually sense a channel until it detects that it's idle. Even then, it will give a propagation delay before starting transmitting in order to make sure that the channel is clear. If an attacker is sending packets on the same channel the authorized device wants to use for transmission, the authorized device will always fail the carrier-sensing and will require to back off. Therefore, the device will know that it's a victim of a denial of service attack.

In the physical layer detection, a legitimate device should be able to distinguish between the normal and abnormal level of noise in a channel. It can do so by collecting enough data of the level of the noise in the network and building a statistical model to use for comparison thus aiding in the detection of a denial of service attack occurrence. A jamming detection technique can also be used to detect jamming. It investigates the relationship between Signal Strength (SS) and Packet Delivery Ratio (PDR).

If SS is high, but PDR is low; a legitimate user may assume that it's being jammed unless one of its neighbors has high SS and PDR. This technique is named as Signal Strength Consistency Checks. Location Consistency Checks can also be used to detect jamming. Here the location of the neighbors is important and can be acquired through GPS and then advertised by each node. A node is jammed when its neighbors should have been delivered at least a minimal amount of packets. A node will check its PDR and will decide if the PDR is consistent with

what it should be given the location of its neighboring nodes. Theoretically, neighboring nodes that are close to a particular node should have high PDR values, and if all nearby neighbors have low PDR values this may lead to concluding that this user is either being jammed or have poor link quality with its neighbors.

After detection of jamming, strategies that can be used to defend against jamming (Denial of service) are: Channel surfing or frequency hopping: In channel surfing and frequency hopping communicators agree to use a different channel once a denial of service attack is detected through any of the detection techniques mentioned above. Spatial retreat: In spatial retreat authorized users change their location to escape the interference range forced upon by the attacker. However the users along with leaving the region with certainly, where the attacker is located they must stay within range of each other to continue communication.

### 5.4Defending against spectrum sensing data falsification attack

[1] To defend against SSDF or Byzantine attack the Byzantine attacker needs to be detected. A possible detection mechanism is to identify Byzantine attackers by counting mismatches between their local decisions and the global decision at the fusion center over a time window and then removing the Byzantines from the data fusion process. The technique proved to be robust against Byzantine attacks and it successfully removed the Byzantines in a very short time span. Neyman-Pearson test is another technique of detecting byzantine attack. Neyman-Pearson method requires definition of either a maximum acceptable probability of false alarm or a maximum acceptable probability of miss detection. It works by guarantying that the other probability is minimized, whereas the defined probability is acceptable. Neyman-Pearson test requires the knowledge of the a priori conditional probabilities of the local sensing. A malicious user detection algorithm that calculates the suspicious level of secondary users based on their past reports is also efficient. The algorithm calculates trust values as well as consistency values that are used to eliminate the malicious users' influence on the primary user detection results. The results gives indication that even a single malicious user is quite capable of degrading the performance of collaborative sensing. The trust value indicator can effectively distinguish between honest users and malicious secondary users. When a good user suddenly turns bad, the technique quickly reduces the trust value of the user. If the user behaves badly for a few times, its trust value recovers only after a large number of good behaviors. If the bad behavior is consistent, the trust value becomes almost impossible to recover. The technique has shown satisfactory performance in some scenarios but its performance is yet to be analytically tested.

### 5.5Defending against control channel saturation and selfish channel negotiation attacks

To reduce CCSD and SCN a trusted architecture can be adapted where any suspicious CR host will be monitored and evaluated by its neighbors. A neighbor can then perform a sequential analysis on the set of data that it has observed and come to the conclusion whether it is misbehaving or not. The Sequential Probability Ratio Test can be used for that purpose as it has proven its efficiency in terms of detection time.

### 5.6Defending against sinkhole attack

[1] A sinkhole attack is hard to detect because it exploits the very design of the routing protocol and network architecture. There are however certain protocols that are well protected against sinkhole attack, they are geographic routing protocols. Geographic routing protocols build up a topology on demand using only local communications and information without base station initiation. Thus, traffic will be routed to the physical location of the base station and will be difficult to lure it to go elsewhere to create a sinkhole.

### 5.7Defending against HELLO flood attack

[1] To counteract the danger of HELLO flood attacks, a symmetric key should be shared with a trusted base station. The base station will act as a Trusted Third Party like in Kerberos and encourage the foundation of session keys between gatherings in the system with a specific end goal to secure their communication.

However certain points must be remembered:
(i) Two nodes may use the session key to verify each other’s identity, authenticate and encrypt the link between them.
(ii) To prevent intruders from creating a session key with every node on the network, the number of shared keys must be limited.
(iii) A node claiming to be the neighbor of many nodes in the network must raise an alarm.

### 5.8Defending against lion attack

[1] In order to cope up with lion attack the TCP protocol must be made aware of what is happening in

the physical layer by employing cross-layer data sharing between physical/ link and transport layers. Thus the CRN devices will be able to fix TCP connection parameters during frequency handoffs and adapt them to the new network conditions following the handoff. To secure the control data in order to prevent the attacker from eavesdropping current and future actions of the CRN, a group key management (GKM) can then be used to allow CRN members to encrypt, decrypt and authenticate themselves. A cross-layer IDSs specifically adapted to CRNs can be used to find the source of the attack provided it is existent.

## 6. Conclusion and future work

The survey gives a clear picture about the classification of cognitive radio network architectures and the various layers constituting a cognitive radio network. It gives an idea regarding the various cross layer frameworks designed to improve the quality of service for the secondary users. Cross layer designs promises more efficient spectrum aware communication provided research work is carried out in the cross layer designs. The attacks on various layers pertaining to cognitive radio networks too are recent and important, targeting CRNs. The countermeasures suggested are sure to be effective enough, giving a secured CRN. As newer attacks come up so will other measures be developed to mitigate them. This relies on the future work in the field of security in cognitive radio networks, its threats and mitigation.

## Acknowledgment

I being the author am very much grateful to the Department of Computer Science for giving me an opportunity to do the research work on cognitive radio network architectures and attacks on cognitive radio networks. I am also grateful to Dr. Fr. John Felix Raj for giving all inspiration and support for carrying out research work in Computer Science and Engineering.

## Conflicts of interest

The author has no conflicts of interest to declare.

## References

[1] El-Hajj W, Safa H, Guizani M. Survey of security issues in cognitive radio networks. Journal of Internet Technology. 2011; 12(2):181-98.

[2] Khare A, Saxena M, Thakur RS, Chourasia K. Attacks & preventions of cognitive radio network-a survey. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 2013; 2(3):1002-6.

[3] Singh JS, Singh J, Kang AS. Cognitive radio: state of research domain in next generation wireless networks-a critical analysis. International Journal of Computer Applications. 2013; 74(10):1-9.

[4] Yuehong G.Thesis for the degree of Philosophiae Doctor. Trondheim. 2012.

[5] Shine Let G, Josemin Bala G. a review of cross-layer design in dynamic spectrum access for cognitive radio networks. Journal of Computing and Information Technology. 2014; 22(1):21-9.

**Kaustav Ghosh** Student of M.Sc. Computer Science, Department of Computer Science. Currently doing research work in the area of Cognitive Radio. Educational institute: St. Xavier's College (Autonomous). 30 Park Street, Kolkata-700016, India.