A Survey on Security Aspects of Cross Layer Design in Cognitive Network

Rittika Guha[#], Priti Prasad[##],Sunit Acharya[*],
Prof. Deep Malya Mukhopadhyay[@], Prof. (Dr.) Anindya Jyoti Pal[**]

[#,*, ##]*Student,Department of Information Technology, Heritage Institute of Technology, Kolkata*
[@, ,**]*Assistant Professor, Department of Information Technology, Heritage Institute of Technology, Kolkata*

Abstract – **Cognitive Radio Network is a new and upcoming technology which allows unlicensed secondary users to use temporarily available spectrum bands of licensed users in the network without any kind of interference with the transmission of data by the licensed users. The spectrum usage in the cognitive radio network is prone to attacks and threats which can be used by unwanted users as unlicensed users are allowed on the network. The previous works dedicated to the security aspects in cognitive radio networks are mainly focused on the security of individual network layers. Cross layer design is a new approach to increase the efficiency in spectrum usage and the working of a CR network. It supports the mechanism of information exchange in between the network layers to improve the network efficiency. In the paper, we will be working with the security aspects and threats to the cross layer design.**

Keywords – Cognitive Radio Network, Cross Layer Design, Security.

I. INTRODUCTION

The fixed spectrum assignment policy of the government creates licensed users who are the authorized users of the spectrum. This spectrum is allotted to the licensed users on a long term basis. Additionally, the large portions of the assigned spectrum are used sporadically as in Fig 1[1], creating spectrum holes, also known as white spaces. The spectrum usage remains concentrated only in certain portions of the available spectrum while a large amount of the spectrum are not utilized. As stated by the Federal Communications Commission (FCC), the utilization of the assigned spectrum varies both temporally and geographically and ranges from 15% to 85%[1]. This fixed spectrum assignment policy proved to be effective in the past, but due to the exponential increment in the number of mobile users in the recent years, the need to access the limited spectrum also increased. Due to the inefficiency in the spectrum usage and the limited availability of the spectrum it became necessary to adapt a new spectrum usage policy to exploit the wireless networks opportunistically. The proposed technique to solve these problems is Dynamic Spectrum Access Policy[1].

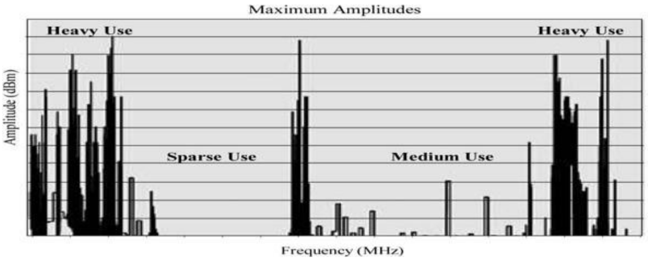

Fig. 1. Spectrum utilization.

The Dynamic Spectrum Access Policy was adopted and applied in a radio network named Cognitive Radio Network which was first presented by Mitola and Maguire in 1999[2]. The Cognitive Radio Network allowed the unlicensed users to use the inactive and empty channels of the licensed users in the same CR network. A cognitive network has an intelligent cognitive process that perceives the current network conditions and theparameters, and thereafter engages itself in planning, deciding and acting wisely in order to adapt to the immediate network changes. The CR network also has the ability to adapt from these changes, learn and refer to them for taking decisions in the future, keeping in mind the end-to-end goals of the communication network.

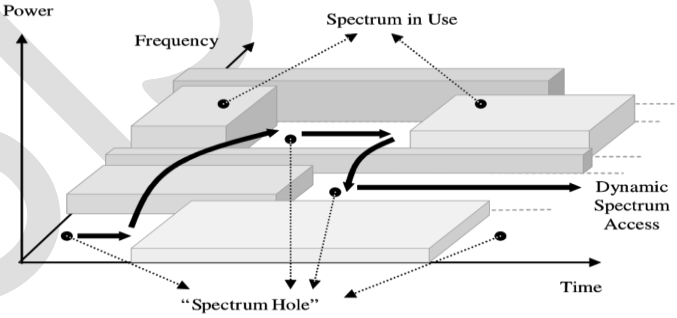

Fig 2. Dynamic Spectrum Access in Cognitive Network

The CR Network is able to find the solution for the spectrum inefficiency problem as it allows unlicensed users to penetrate into licensed bands of spectrum and use them at the same time, without causing any kind of interference. The licensed users are termed as primary users and the unlicensed as the secondary users. The primary users use only a portion of the licensed band, while the remaining is kept idle.Cognitive Radio Network allows the secondary users to use these idle spectral bands to improve the efficiency of the network.This is achieved through constant monitoring of the licensed bands by the secondary users in order to detect empty spaces or holes in the spectrumand then accessing and transmitting packets through thesespaces without causing any sort of interference with the primary users.

When the licensed bands are in an active state, then it is always better for the secondary users to avoid that channel. Further, if a secondary user senses the presence of primary user in the band which it is currently using then it needs to vacate the particular band and move to a different spectrum hole for carrying on with its transmission and communication in the CR Network as shown in Fig 2[1]. This hopping movement of the secondary users is achieved through spectrum sensing, spectrum management, spectrum sharing and spectrum mobility. Meanwhile, at the same time specific security measures should also be adopted so that any kind of misuse of the available spectrum bandwidth can be prevented.

II. BRIEF ARCHITECTURE OF COGNITIVE RADIO NETWORK

As stated above, the total available spectrum is divided and allocated to the licensed users as per their needs. In most scenarios it is found that a part of the spectrum remains unlicensed, as well as the licensed band of the spectrum also remains idle for a significant amount of time. This leads to the poor utilization of the spectral bandwidth leading to a decrease in the network efficiency. Based on these reasons, a network with cognitive capabilities have to be deployed. The components which make up the cognitive network are mainly a Primary Network and a Secondary Network as shown in Fig 3[1]. The prime elements of both these networks are stated below:

A. Primary Network: The users having exclusive right over the spectrum through the license from the government are termed as primary users. The cellular and the TV broadcast networks are popular examples of the primary users. The primary network is made up of the following components:

1) Primary User—The licensed or the primary users in the cognitive network have the license to work and operate in a specific spectrum band as allocated by the government. The operation of the primary user can only be controlled by the primary base station which should not be affected by the actions of any kind of secondary users. These users do not require any kind of adaption or modification of their configuration in order to co-exist along with the secondary user in the Cognitive Radio Network.

2) Primary Base-Station -- The licensed or the primary base station resembles the base-station transceiver system (BTS) in a cellular network. It has a fixed infrastructure with a spectrum license. By the principle of BTS, these base-stations do not have the capability of spectrum sharing. But looking into the needs of the present situation, they can be modified considerably so that these stations can support the age-old techniques of wireless communication as well as operate with the trespassing nature of the secondary users.

B. Secondary Network: The secondary network or the unlicensed network does not possess the desired band in which they wants to operate. Hence, this network works only in an opportunistic manner through Dynamic Spectrum Access which is achieved by following the cognitive cycle as mentioned in Fig 4[1]. The secondary network can either be deployed as an Ad Hoc Network or as an Infrastructure Network or both as shown in Fig 4. The unlicensed network of the secondary users are made up of the following components:

1) Secondary User – Also known as Cognitive Radio User and Unlicensed User. The CR User does not have any kind of spectrum license. Hence, it requires specific configurations to be able to access the licensed spectrum bandwidths of the primary users.

2) Secondary Base-Station – The Secondary Base-Station or the unlicensed base station is the infrastructure supporting the cognitive capabilities like spectrum sensing, spectrum mobility, spectrum sharing and spectrum management. These base station also provide single hop

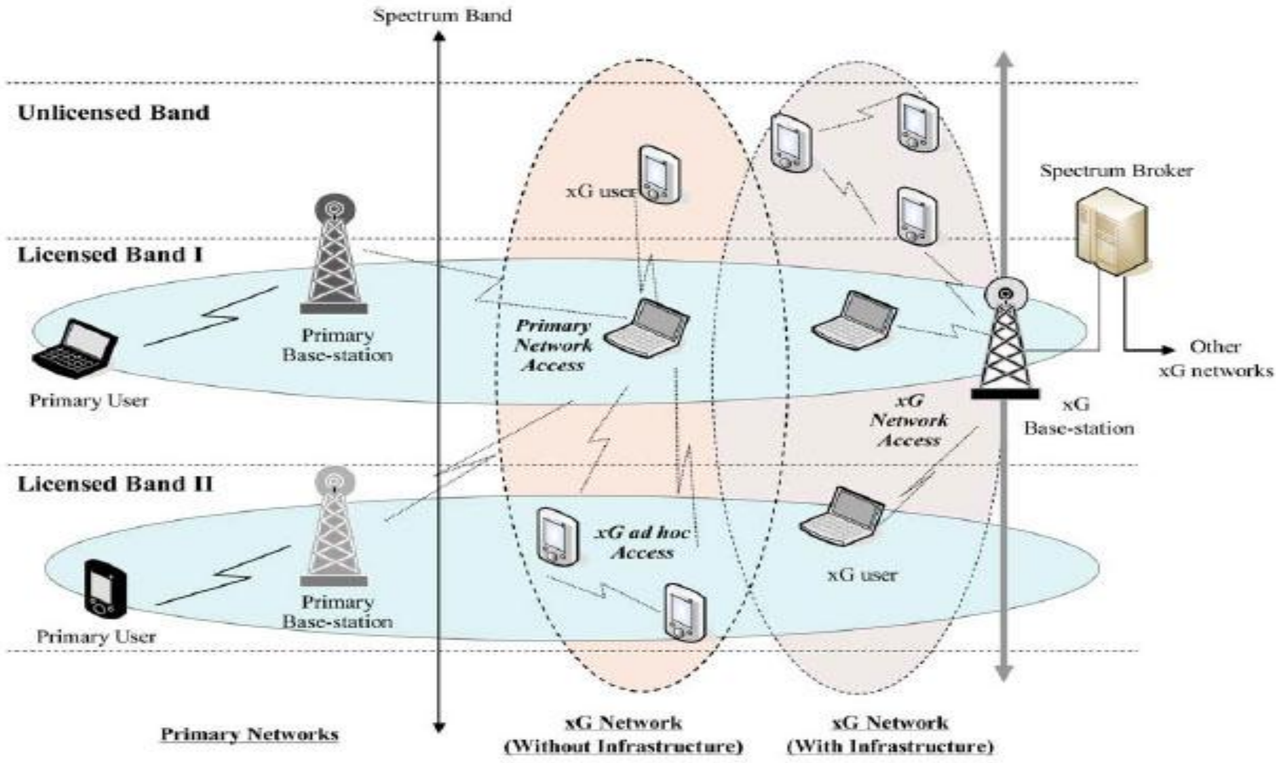

Fig 3. Cognitive Radio Network Architecture

connection to the unlicensed users through which the unlicensed users can access the desired spectrum.

3) Spectrum Broker – It is the central network backbone for the secondary networks and is responsible for catalyzing the spectrum sharing process amongst different secondary unlicensed users. A Spectrum Broker when connected to two or more secondary networks in a CRN, it allows the coexistence of multiple secondary networks together through efficient spectrum management.

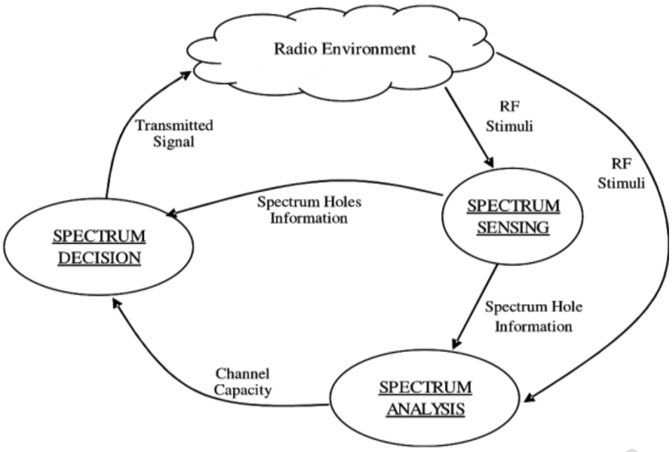

Fig 4. Cognitive Cycle

III. PROBLEMS LEADING TO ADOPTION OF A CROSS LAYER DESIGN

The properties of the spectrum band in use and the characteristic functions of the secondary networks are directly interconnected and also depend directly on each other. This kind of direct dependency calls for the application of design architectures like cross layer design for implementing the secondary Ad Hoc Networks. More specifically, the changes occurred in the network parameters due to spectrum mobility and consecutive selection of a different spectrum bandwidth asks for minute consideration in the designing of the network architecture along with the communication protocols. On the whole, such architecture must be able to support the cognitive capabilities like spectrum sensing, spectrum management and spectrum handoff in a collaborative manner. Based on this concept, we proactively identify the problems with the existing system which can be improved with the proper implementation of cross layer design architecture in Cognitive Radio Network.

A. Challenges in Spectrum Management: The secondary users operate dynamically to adopt the wireless channel parameters. More precisely, the change in parametersof one protocol demands a change in the parameters of other protocols. Hence, the change penetrates across multiple layers. This provides enough evidence for the need of deploying a cross layered architecture which will consider the interdependencies amongst the media access layer, transport layer and the application layer. At the same point of time the cross layer spectrum management can maintain and decide the appropriate spectrum band for transmission with proper QoS Standards and spectrum sensing methodology.

B. Challenges in Spectrum Handoff: Spectrum handoff is closely related and influenced by the dynamic use of the spectral band. The changes in the PHY and MAC layer parameters can initiate a spectrum handoff which has adverse effect on the channel parameters like path loss, interference, link layer delay, and many more. Moreover, spectrum handoff also introduces latency in the network which is undesirable. But at the same time spectrum handoff is requested by the users for a better quality of communication. Since we need to maintain an overall QoS, all the layers must have the knowledge of any kind of change introduced in the protocol stack due to this spectrum handoff. This kind of requirement can only be met through a cross layered design in which there are no strict boundaries among the layers thus, allowing parameters to bepassed from one layer to the other in order to adapt to the change in the cognitive environment.

C. Challenges in Upper Layers: The secondary users have to incorporate a multi-hop communication method to operate efficiently for which it needs to have the topology information as well as the information about the availability of sensed spectrums. Based on these data, the secondary users can decide the routing mechanism. Further, if a packet loss occurs due to interference from primary user, the routing algorithm must know how to differentiate between a link-failure and a node-failure. Generally, a link-failure introduces end-to-end latency in the network leading to degradation in the QoS. Finally, for successful transmission a re-routing needs to be performed. This mechanism leads to variable packet loss rates in the secondary network and introduces access delay as the spectrum has to be sensed and re-routing has to be performed. As a result, the Round Trip Time of the connection is affected greatly, degrading the performance factors of the transport layer protocols. Thus, this encourages the implementation of cross-layer architecture with a cooperative approach across the different communication layers.

D. Challenges in Spectrum Sharing: Spectrum sharing in dependent on the information gathered by Spectrum Sensing in the PHY layer. Moreover, these two activities must act in a cooperative manner in a secondary cognitive radio network. If this behavior is adopted, then there arise two shortcomings.

First, the CR Network must be able to prevent interference with the primary users. Network interference mainly occurs at a receiver, while on the other hand, spectrum scanning in performed on the transmitter end. In order to maintain a cooperative nature, the network must be modified so that it can consider both the interference caused at the transmitter end as well as at the receiver end. This increases the communication overhead and leads to the degradation of the system performance. Along with spectrum sensing, equally modified methodology must be acquired for spectrum sharing between the secondary users in the CR Network.Second, spectrum sensing is limited to a certain portion of the total available bandwidth. This is mainly because the secondary users cannot sense the whole spectrum all at once since it is time consuming. Also, spectrum sensing and communication has to be collaborated to obtain optimal efficiency. This could be performed through a greedy approach where limited spectrum sensing is done optimally so that the empty spectrum band chosen can be the best available option for the next hop in the secondary network. However, optimally chosen spectrum bands were robust in nature and also prone to erroneous results. Hence in such a situation a cross layer design has to be employed so that, a spectrum is sensed by the MAC layer only when a call is initiated by the application layer in the network and subsequently the parameters in the PHY layers can be updated.

IV. CROSS LAYER DESIGN ARCHITECTURE

The existing communication model or the protocol stack model was highly rigid and strict i.e. each layer in the model was only responsible and worried about the layer just above it or just below it as in Fig 5[7]. This lead to the problems as discussed above.An optimized wireless network can be obtained through the consideration of both the challenges from the communication layers as well as the QoS Standards. Parameters like rate of packet loss, energy efficiency and throughput of the CR Network can be modified and adapted in accordance with the requirements and necessity of the channel and current spectral bandwidth conditions. In order to achieve this kind of optimization, the information and knowledge about the network gathered through spectrum sensing and spectrum management techniques must be collaborated and shared amongst all the layers in the communication system. This sharing of information in between the layers of the communication model for achieving better optimal results in terms of efficiency, throughput and latency in the cognitive radio network is termed as cross layer communication technology. While the network topology which is built based upon this cross layer technology is referred to as a cross layer[12] [14] design in CR Networks.

V. CROSS LAYER SECURITY ATTACKS

A cross-layer attack is a collection of attack activities thatare conducted coordinately in multiple network layers in order to achieve specific attack goals [3]. We can also state that the cross layer attacks are simple modifications of the effects they have on a single layer to multiple layers across the communication model. The different security threats can be visualized from Fig 6[13].

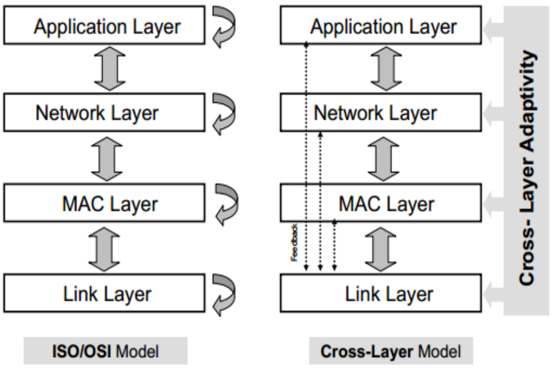

Fig 5. Cross Layer Architecture (right) versus ISO/OSI Communication Model (left)

A. Attacks in The Physical Layer: While a cross layer design optimizes the efficiency and working principle of the Cognitive Radio Network, it also introduces cross layer attack. Cross layer design in Cognitive Radio Environment allows consideration of multiple channel parameters at the same time. On the other hand this kind of collaboration between the different layers can lead to new problems. In a cross layered approach when a frequency change occurs due to the change in the frequency band for sustainable data transmission, a certain degree of delay is introduced. This kind of delay attracts malicious attackers in the PHY layer. Such an attack is known as Lure attack problem of Cognitive Radio Network. In this attack, a malicious node which is introduced in the channel starts inputting false information regarding the spectrum availability and forces the requesting nodes for data transmission through this false pathway. This kind of falsification in routing mechanism leads to unnecessary packet loss and degradation in the communication performance factors of the network. As the PHY layer parameters are updated with false information, it also forces the upper layer parameters to be modified accordingly, thus leading the attack in a single layer upwards through the communication layers. This kind of falsification leads to cross layer Luring Effect[4] as it lures the nodes in the cognitive network to update its parameters across all the layers consecutively on the basis of a false estimation as well as is responsible for frequency jamming[3], [4], [5].

B. Attacks in The Mac Layer: The main problem in the Media Access Layer is that of congestion in the network, but the MAC Layer is self-sufficient in protecting itself from such problems. However, the mechanisms incorporated to deal with such problems might be used by the attackers to degrade the quality of communication in the MAC layer. The MAC Layer mechanism states that any signal can pass through the MAC Layer only after an ACK signal is received by the sender from the receiver. But if a failure occurs in this layer, it leads to a disruption in the Network Layer. Taking this opportunity, the attacker isolates several nodes in the CR Network by disabling the MAC Layer properties.

The MAC Layer can be affected by several kinds of security attacks. The attacker might be keeping the spectrum channel in use busy all the time, so that the normal nodes are unable to access them. This ultimately leads to DoS[3], [5] attack in the requesting node. Due to this kind of situation, a queue is formed out of the demanding nodes for channel access. Finally the heavily loaded node forcefully captures the channel and starts to transmit data continuously making the neighbors to move backward.

As per the above mentioned discussion, nodes are classified into three broad categories in the MAC Layer[5]. Firstly, a node is said to be normal if it obeys the rules of the MAC Layer protocols and does not act selfishly. Secondly, it is malicious if it engages in communication with other malicious nodes of the network, leading to DoS in multiple nodes of the network. Lastly, the node can be misbehaving when it operates in a suspicious manner and tries to disrupt the normal working of the network by seeking false priority in the network. These nodes start to change and modify themselves from a malicious node to a misbehaving node so that, they can maintain the priority in the network. This attack leads to jamming of the network and disruption of the routing pathways in the CR Network across the MAC Layer as well as the Network Layer.

C. Attacks in The Network Layer: The network layer in the cognitive radio network is prone to the Sink-Hole Attack[5], [12]. In this attack, the attacker broadcasts a message to the other cognitive nodes that it forms the probable best cost effective pathway in the current network. Consequently, the nodes working at the network layer chooses this false routing path to send the data packets. These data packets are nothing else other than TCP packets. Further, the attacker takes the notion of selective forwarding in the transport layer, thereby absorbing a significant number of packets and restricting the same from reaching the destination. This leads to an increase in the retransmission delay in the transport layer protocol and finally causes packet losses. Hence, the total communication performance in the CR Network is degraded due to this cross layered attack which is built in the network layer and effects the transport layer simultaneously.

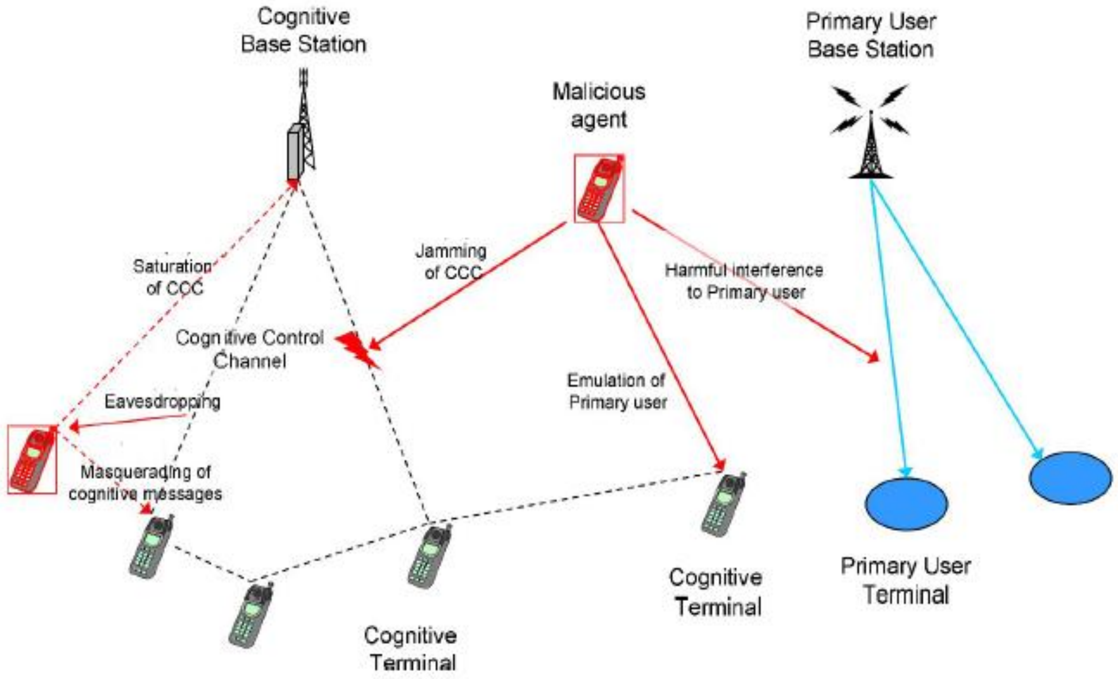
Cognitive Base Station
Primary User Base Station
Malicious agent
Saturation of CCC
Jamming of CCC
Harmful interference to Primary user
Cogn itive Control Channel
Emulation of Primary user
Eavesdropping
Masquerading of cognitive messages
Cognitive Terminal
Primary User Terminal
Cognitive Terminal

Fig 6. Security Threats in Cognitive Radio Network

D. Attacks in The Transport Layer: The lion attack [9], [12] mainly resides in the PHY Layer through the traditional Primary User Elimination (PUE) attack and targets to break up the TCP Connection at the transport layer. It is a cross layer attack which degrades the TCP performance and forces the CR Nodes to undergo frequency handoffs. During the PUE, all the Secondary users are forced to change their frequency bandwidth in which they are operating. But at the same time, the transport layer is unaware of this handoff, and will go on increasing its retransmission time leading to delay and packet losses unnecessarily.

E. Attacks in The Application Layer: Sybil Attack [11] is a kind of application layer security threat in CR Network. In this, a signal entity operates like multiple entities (Masquerading). It leads to a confusion in the routing layer, as the senders cannot locate the right receiver and at the same point of time the attackers remove the routing pathways from the routing table. This introduces a delay in the routing layer and degrades the QoS. Moreover, the attack in the application layer leads to an adverse effect in the Network layer which is widely responsible for the routing mechanism in the Cognitive Radio Network.

VI. SOLUTIONS FOR THE SECURITY ISSUES IN SINGLE LAYER DESIGN

One of the probable ways to cope up with the security issues in the cross layer design architecture in cognitive radio network is to introduce authentication systems and intrusion detection systems (IDS). Using these systems in a different layer referred to as the security layer, the operations at the other layers can be modified and updated in order to get the optimal result. For instance, if the authentication system and intrusion detection systems operating at the application layer gathers information about the real-time attackers, then this information can be passed onto the lower layers to improve the efficiency and throughput considerably. This can also help to improve the robust nature of the communication network. On the other hand, implementing this kind of systems will make the system more complex and costly, while increasing the time taken for internal processing within a given node. At the same time, it will help in the reduction of communication requirements such as there will not be any need for checking the neighboring nodes, because using these methods will demolish the concept of critical nodes.Such kind of systems can be used in cognitive radio network with limited spectrum bandwidth. The security threats which can be solved and removed from the network using these systems are discussed below:

A. Intrusion Detection: Intrusion Detection Systems (Fig 7[11]) or IDS[8] are used and implemented to test and find the intruded entities in the network which is subjected to any kind of network or application layer attack. The IDS can be implemented with a distributed approach and set to control and monitor the neighboring nodes constantly. This proves to be extremely beneficial in areas like Byzantine[6],[8] routing that includes implementing algorithms for the detection of false information introduced in the network. This approach thus makes the network more robust. Implementation of the IDS in this manner can be referred to as the trust-based approach and can be deployed using hash-chains and digital signatures. But unfortunately, such method proved to be an overhead in the network and occupy large stretches of the available bandwidth unnecessarily. According to recent research works, if an attack is detected in a particular layer then mitigation measurements are required to be implemented in the other layers. The Intrusion Detection Systems can be classified into three categories[11]:

1) Host-Based IDS – Also known HIDS, is used to control and monitor processes in a computer to find any kind of indications regarding misuse. This IDS category has the power of detecting and responding to suspicious activities on its host node. The responsiveness of this kind of IDS is dependent only upon the collected data in the host audit logs.

2) Network-Based IDS (NIDS) – It is used to monitor traffic in network constantly to gather signs of threats. It uses a methodology based on the listening, capturing and examining individual data packets in the network including the header length.

3) Specification based Intrusion Detection – This IDS is a combination of both misuse and anomaly having drawback in the development process as it is manually done.

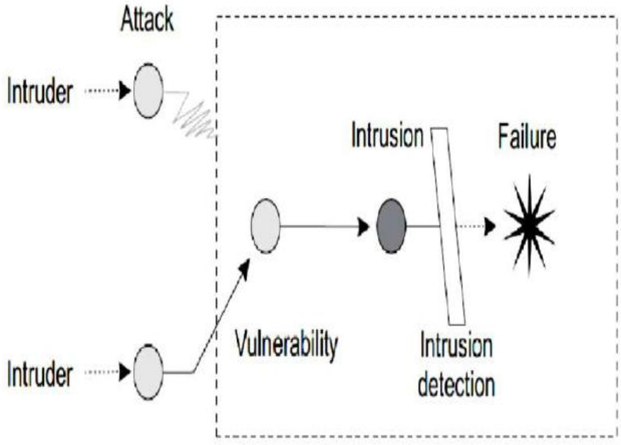

Fig 7. Intrusion Detection System

B. Frequency Hopping: It is used as a security measure against threats like frequency jamming in the physical layer.Here, a node is set to transmit within a certain predefined set of frequencies which follows the nodes that occupy those frequencies. The range of frequency hopping[8] can be set to the application level requirements which can in turn be modified dynamically according to the physical layer parameters. If the range of frequencies is large and spread over a wide area then it proves to be beneficial in this case, because it makes the transmission of the energy from the potential attacker difficult, in turn preventing the demodulation at the receiver.

C. Distributed Authentication: In order to develop a secure Cognitive Radio Network with a Cross Layer Design Implementation one can use the technique of threshold cryptography. Threshold cryptography[8],[13] refers to a security action where every node in the network has access to a common network master key while it provides provisions like issuing of private keys. Here private keys refer to partial certificates which is generated by ‘n’ special nodes in the network. Further, a valid certificate is formed by the combination of ‘k’ partial certificates, this is known as threshold cryptography. This procedure of threshold cryptography is highly popular as because key management is regarded to be much simpler than public key infrastructure. In this approach a network can hold its security up to the threshold value of (k-1) shareholders. Hence, the optimal selection of the nodes in the network is of prime importance. However, such an optimal selection and careful planning can lead to the prevention of unwanted operations by malicious as well as misbehaving nodes in the Cognitive Radio Network.

D. Signal Analysis: This technique is used as a measure of protection form application layer attacks like Sybil attack [11] which is implemented through the masquerading of a secondary node in the network, thereby leading to confusion in routing path and introducing delay in the network through the removal of existing routing paths from the routing table. The signal analysis addresses these unwanted users by recognizing the signals which are not authorized in the network or in the licensed band and hence it stops the secondary users from trying to communicate with these nodes respectively. However, it is possible for an attacker to masquerade the primary or secondary node itself. In such cases, the signal analysis is performed through location verification because of the assumption that the CR Nodes are fixed according to their geographical locations and a trusted source of GPS is used for tracking them.

VII. PROBABLE SOLUTIONS FOR CROSS LAYER ATTACKS

Based on the above solutions for single layer, we are suggesting some of the probable solutions which can implemented in the cross layer architecture to prevent the possible attacks. These are merely based on the idea that the security measures taken for single layered approach might be extended over a cross layer design in Cognitive Radio Network for both Primary and Secondary Users.

Cross Layer Attacks in CR Network	*Probable Solutions*
Physical Layer (Lure Attack)	Implementation of a system (IDS) which will be capable of searching and eliminating any kind of intruder in the network [VI.A]. Using a trustworthy detector (signal analysis) for geographical locations based on central GPS system [VI.D].
MAC Layer (DoS Attack)	It can be resolved using Threshold Cryptography (Distributed Authentication System) which will set security keys for every predefined nodes in the network so that no intruder can communicate with the CR nodes [VI.C].
Network Layer (Sink Hole Attack)	Use a detection process to check the path of routing for the malicious node before transmitting the TCP packets in network. Also an IDS can be implemented in the network layer and set to check the routing path for unwanted intrusion in the transport layer.
Transport Layer (Lion Attack)	The probability of the PUE in the physical layer might be decreased by using the threshold cryptography[VI.C] and signal analysis[VI.D].
Application Layer (Sybil Attack)	Signal Analysis[VI.D] by detection of trustworthy GPS location of the primary and secondary nodes in the Cognitive Radio Network or by checking for intruding nodes periodically (IDS) [VI.A].

VIII. CONCLUSION

Even though the modern cognitive research community emphasizes on the implementation of cross layer architecture, it might bring in several security issues in the network. Bundled with a bunch of threats, there can be disadvantages also like tight coupling, unbridled stack design, loss of modularity and incorrect system implementation leading to an undisciplined cross layered architecture[7],[12]. Such an architecture will surely degrade the networks performance parameters in place of improving the efficiency of the Cognitive Radio Network. While, on the other hand cross layered architecture, if implemented properly maintains adaptability, security, Qos, ease of spectrum mobility and efficient spectrum management procedures over the ISO/OSI model for communication. At the same point of time, efficient measures needs to be undertaken to override breaching of the security in the network because cross layer design relaxes the idea of strict boundary in between the protocol layers, thus making it easier for the attackers to break the network security. These security measures can be adopted through the extension of single layer security measures to the cross layers in CR Network.

REFERENCES

[1]. I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “NeXtgeneration/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[2]. KhaleelHusain,PremalaPatil, “A Survey On Different Cross-Layer Attacks And Their Defenses In Manets”, IJRET: International Journal of Research in Engineering and Technology

[3]. Wenkai Wang and Yan (Lindsay) Sun, Husheng Li, Zhu Han, “Cross-Layer Attack and Defense in Cognitive Radio Networks”.

[4]. Long Tang, Juebo Wu, “Research and Analysis on Cognitive Radio Network Security”, Published Online April 2012 (http://www.SciRP.org/journal/wsn)

[5]. Svetlana Radosavac, Nassir Benammar and John S. Baras, “Cross-layer attacks in wireless ad hoc networks”, 2004 Conference on Information Sciences and Systems, Princeton University, March 17-19, 2004.

[6]. A.Rajaram, Dr.S.Palaniswami, “A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009.

[7]. Cross-Layer Optimizations in Multi-HopAd Hoc Networks, Marco Di Felice, March 2008, Prof. OzalpBabaoglu, Dott. Luciano Bononi.

[8]. K.P.Manikandan, R.Satyaprasad, K.Rajasekhararao, “ A Cross Layered Architecture and Its ProposedSecurity Mechanism to Lessen Attacks Vulnerability in Mobile Ad Hoc Networks, International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011, 1007-1011

[9]. JaydipSen, “Security and Privacy Challenges in Cognitive Wireless Sensor Networks”, *Innovation Lab, Tata Consultancy Services Ltd., Kolkata, India*

[10]. Mr. Vishal S. Badgujar, Prof. Sudhir N. Dhage, “Effect OfBlackhole Intrusion In Wireless Networks”, International Journal of Computer Engineering and Applications, Volume VII, Issue III

[11]. Sangeeta Bhatti, Prof Meenakshi Sharma, “A Review of Sybil Attack in Mobile Ad-hoc Network”, International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE) Volume 1, Special Issue

[12]. GeethapriyaThamilarasu, Ramalingam Sridhar, “Exploring Cross-layer techniques for Security:Challenges and Opportunities in Wireless Networks”.

[13]. GianmarcoBaldini, TajSturman, Abdur Rahim Biswas, RuedigerLeschhorn, Gy¨oz¨oG´odor, Michael Street, “Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead”, IEEE communications surveys & tutorials, vol. 14, no. 2, second quarter 2012

[14]. Mr.M.D.Nikose, “A Review Of Cross Layer Design”, International Journal of Emerging Trends in Engineering & Technology (IJETET)Vol. 02, No. 01, 2013