Comprehensive Survey On Network And Cross Layers Of Cognitive Radio Networks

Mahesh kumar N, Dr. Siddesh G K

Abstract: Nowadays growth in wireless communication has increased the demand for wireless radio spectrum to utilize many social and individual benefits. Hence the radio spectrum allocation and utilization is also an important task. The CRN is a novel technology that promises to solve this problem by allowing unlicensed user to access the radio spectrum without any interference to licensed user. Due to this flexibility cognitive radios are explore to different types of threats and security attacks. The aim of this survey is to investigate different attacks applicable to the Network and Cross layers of cognitive radio and provide an overview of them based on layer wise functionalities. In addition, this paper describes and compares recent defense techniques related to each attack, that could be faced by any wireless networks.

Index Terms: Cognitive Radio Network, Security, Network Layer, Cross Layer, Attacks, Countermeasures

1. INTRODUCTION

Wireless communication has created a incredible revolution in the world, with a result an exponential increase in wireless communication devices and their usage. This causes an exponential increasing demand for more radio spectrum. But there is an inefficiently utilization of the radio spectrum band due to static spectrum allocation policy adopted by the governments. Hence, Federal Communication Commission (FCC), approved new guidelines to allow unlicensed users to utilize the underutilized spectrum reserved for wireless broadband services [1]. These encouraged researchers to develop a new spectrum sharing technology to utilize underutilized spectrum bands called white spaces. To solve this underutilized spectrum band problem the cognitive radio technology is developed in the year 1998 [2]. Cognitive Radio Network (CRN) is promising technology that adapt to changes in their environmental conditions to make a better usage of the radio spectrum [3]. Cognitive Radios are smart radios to utilize spectrum efficiently perform the following four basic operations.

a) Sensing the Spectrum: Detecting spectrum white space.
b) Managing the Spectrum: Selecting the best frequency bands.
c) Sharing the Spectrum: Coordinating spectrum usages with other users (coordinate access to this channel with other users).
d) Mobility the Spectrum: Vacate the channel when a primary user is detected

- *Mahesh kumar N, Department of Electronics and Communication, Dayananda Sagar college of Engineering, Bengaluru, India-560078, mkumar.n19@gmail.com*
- *Department of Electronics and Communication, JSS Academy of Technical Education, Bengaluru, India-560060, siddeshgundagatti@gmail.com.*

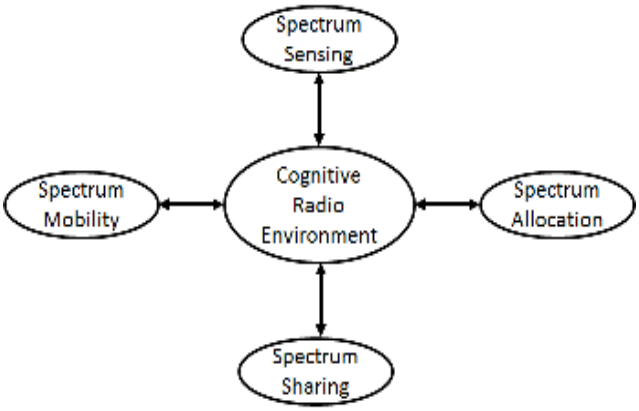

Fig.1 *Cognitive Radio Life Cycle*

CR Networks solve the spectrum utilization problem by allowing unlicensed users to access licensed users spectrum bands without any interference. Due to this flexibility, CR Networks are exposed to different types of security threats and attacks from the unauthorized users, and this causes severe performance degradation of the network. There are various detection and mitigation techniques to protect the cognitive radio networks. In this paper, we mainly focus on Network layer and cross layer attacks of cognitive radio networks and compares recent defense techniques related to each attack. The remainder of the paper is organized in the following manner: in Section II Layer wise attacks in CRN. In Section III: brief about the Network layer attacks and their existing detection techniques and countermeasures. Section IV: brief about the Cross layer attacks and their existing detection techniques and countermeasures. Section V concludes the paper.

1. Cognitive Radio Networks Attacks andcountermeasures:
In this section, we mainly focusing on different types of security attacks specially targeting at cognitive radio networks and we categorized the security attacks based on the layers they are targeting as shown in the Fig.2 [4]. Primary User Emulation Attack, Jamming and spoofing Attacks, Objective function Attack (OFA), Secondary user overlapping attack in the Physical Layer. Spectrum Sensing Data Falsification Attack (SSDF), Biased Utility Attacks, Control Channel Jamming Attack, Asynchronously Sensing Attack in the Link

Layer (MAC layer). Hello flood attack, Wormhole Attack, Sinkhole attack, Sybil Attack in the Network layer. Lion Attack. Jellyfish Attack, Routing Information Jamming and Small Bakeoff Window in the Cross Layer.

2. Taxonomy of Network layer attacks:
This layer is responsible for routing of packets between source and destination, possibly across multiple networks (channels). Attacks in cognitive radio network targeted network layer functions mainly on routing operations by posting the wrong path messages [5]. This causes the collision and leads to drop packets in the network. In this section we mainly discuss an overview of different attacks, which are targeting the network layer. But in this work we are addressing few attacks and their countermeasures.

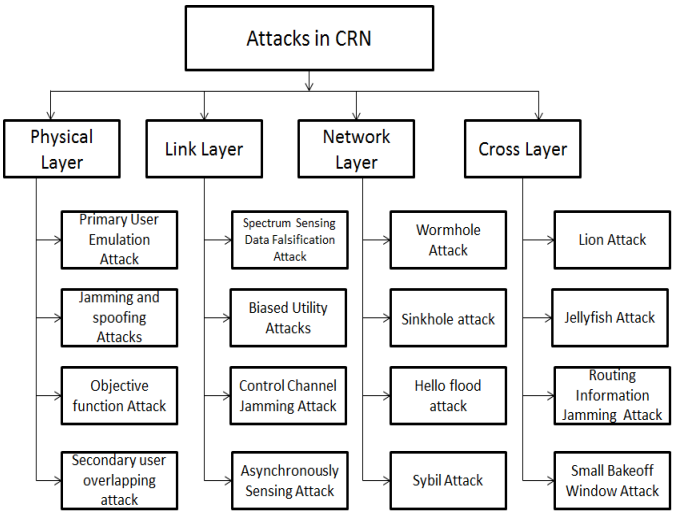

Fig.2 *Attacks in CRNs.*

1.1 Wormhole attack:

The wormhole attack is one of the most severe attacks in CRN. This attack can overcome the confidentiality and authenticity communication. Here one of the malicious nodes (attacker) transmits the messages over low idleness link or captures the traffic at one side of the network and tunnels them to other malicious node (attacker) at other side of the network. The attacker can modify the packets and this causes degradation of network performance [6]. In this example as shown in fig.3, the source node 1 starts a route discovery to destination node 8, by broadcasting a RREQ on all accessible routes. The nodes 2 and 7 are two malicious nodes. Once the node 2 receives any packets, it forwards to node 7 over the tunneling link. The malicious node 7 retransmits the received RREQ packet to the node 8. This RREQ packet reaches the node 8 first, because it is sent through a rapid link. Once the RREQ packet reaches the destination node, it generates a RREP packet and sent to the node 1, through the same tunneling link. Subsequently, all the communication between the source node and destination node go through the same malicious link. Table 1 summarizes the Counter measure for wormhole attack

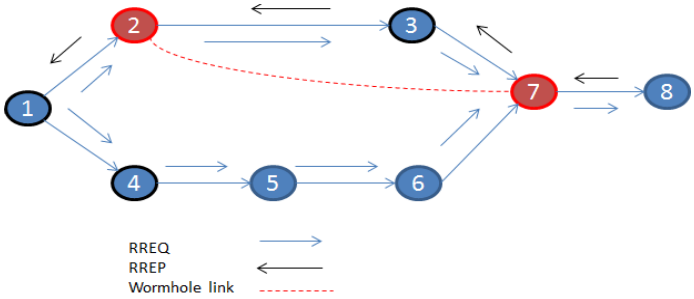

Fig.3. *Wormhole Attack*

Table 1 *summarizes the Counter measure for wormhole attack*:

Approach	Proposed Solution	Advantages	Limitations
Absolute Deviation Statistical Approach Sayan Majumder et al [7]	Time delay calculation between sent and received packets. .	• Less computation overhead. • Light Weight • Robustness of statistical approach • It doesn't require any extra hardware.	This algorithm takes more computational time to avoid wormhole attack.
A scalable and distributed scheme Jayashree et al [8]	They proposed sequential probability ratio test.	• No additional resource requirement • Detection is faster with increasing mobility.	System Overhead in terms of communication, computation, and storage.
Packet leashes Yih-Chun Hu et al [9]	• Geographical Leashes • Temporal Leashes • These detection techniques based on location and time based scheme.	• Clock synchronization not required. • It is highly efficient.	• Limitation of GPS technology. • Increase Computation and network Overhead
Directional Antennas L. Hu and D. Evans [10]	They proposed a cooperative protocol.	• Less expensive • Efficient use of energy and bandwidth	• Required directional antenna. • Directional errors are possible.
Digital Signature Pallavi Sharma et all [11]	Cryptographic technique	• Packet delivery ratio is high. • It doesn't requires any special hardware and synchronized clocks	• Network overhead is also increased • This solution is best suited for traditional networks.

Neighbour node analysis Sweety Goyal et all [12]	Neighbour Discovery Approach	• Through put is increase and also provide better efficiency.	• Not used for large network • This algorithm could not find wormhole, when multiple wormholes are in network.
DelPHI Technique Lui K.-S., et all [13]	This Technique is based on the calculation of (delay/hop) value of disjoint paths	• Synchronization doesn't needed • It does not need any extra hardware or tight time synchronization	• QOS is low because of more delay • The message overhead

1.2 Sinkhole attack:

Sinkhole Attack (SA): The sinkhole attacker can advertise itself as the best path or the shortest route to their intended destinations. This behavior of attacker urges neighboring nodes, which influences neighboring nodes to utilize this as the shortest route to communicate their packets. When attacker receives packets from neighboring nodes it can either modify the information or it can drop the packets. The attacker can begin the attack by building a trust base. The attacker is superior so that it uses its power to transform any information directly to the base station [14].

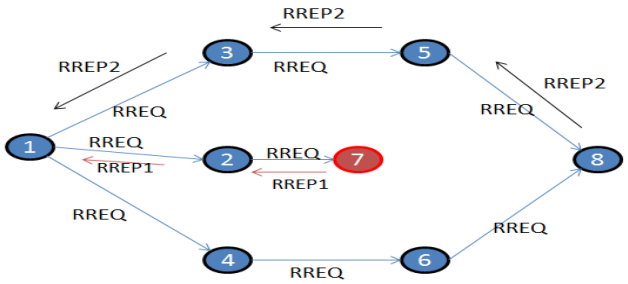

Fig.4. *Sinkhole attack*

Fig. 4, shows an example of sinkhole attack that affects AODV routing protocol in CRN, In AODV routing protocol the source node sends an RREQ request packet to all possible routes to find destination node. The destination node will send RREP packet after it receives RREQ. In this example source node 1 broadcast RREQ packets, nodes 2, 3 and 4 received RREQ. They rebroadcast RREQ and it is received by their neighbor nodes 5, 6 and also attacker node 7. An attacker node 7 sends RREP with maximum destination sequence number and minimum hop counts to source node 1. But source node 1 receives one more RREP packet that comes from the original destination via path 8 to 5 to 3 to 1. This indicates that a malicious node exists in the network.

Table: *summarizes the Counter measure for sinkhole* attack:

Approach	Proposed Solution	Advantages	Limitations
Rule Based. Krontiris et al [15]	Based on Intrusion detection system(IDS)	The proposed algorithm is more secure and robust.	Storage and network overhead
Anomaly based. Sharmila,S. et al [16]	Message digest algorithm technique is used.	This algorithm achieve data integrity and authenticity	Throughput, Network overhead and communication cost was not mentioned.
A non cryptographic Sheela D, et al [17]	Using mobile agent to defend against this attack	Mobile agent has enough power to detect modification, it uses dummy data.	It is used only in Mobile wireless sensor network
Statistical based Chen et al [18]	They proposed statistical GRSh (Girshick-RubinShyriaev)–based algorithm	This technique detect malicious node in short time. Low false positive rate	Base station decides which node is malicious node. Assumption-base station is trustworthy
DSR protocol and watchdog Sergio Marti et al	DSR protocol	Techniques increase throughput by 17% .	Excessive overhead. Failed to detect malicious nodes in the high mobility nodes .

1.2 Hello flood attack:

In Wireless communication networks, packets transaction between the similar behavior nodes involves the identification of neighbor nodes by broadcasting the hello packets periodically. These hello packets are used to establish the bidirectional authentication for information exchange. A hello flood attacker takes benefit of this approach, sends the hello packets over the established channel, which is more eminent and noteworthy. Neighbor nodes trust the false hello packets by assuming as it is from neighbor node and transmits their entire packets through this malicious node. Thus, forwarded packets are lost due to the intervention of foreign node [19]. Table 3 summarizes the Counter measure for Hello flood attack In figure 5 shows a Hello flood attack, attacker node A, broadcasts hello packets to convince other nodes in the network, that they are neighbors of A. Although some nodes like 6, 8, 9 and 7 are far away from this node A. They think A is their neighbor and try to send packets through it, which results in wastage of energy and data loss. To counter this attack, it is possible to use the mechanism of authentication by a third node.

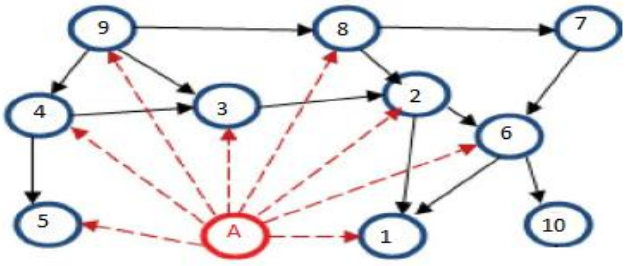

Fig.5: *Hello flood attack*

Table 3 *summarizes the Counter measure for Hello flood attack:*

Approach	Proposed Solution	Advantages	Limitations
Adaptive Detection H. Khosravi et al [19]	IDS based on neighborhood Alpha-Beta Filtering	High packet delivery ratio and low delay This solution also detects collusion attack with an acceptable detection rate.	High false positive ratio
Signal Strength and Geographical information Virendra Pal Singh et al [20]	Non-cryptography, Signal Strength and Geographical information based Approach	Requires less computational power, Packet delivery ratio is more	Network overhead is high. It is not energy efficient
LEACH Protocol Shikha Magotra et al [21]	Non-cryptographic solution and Received Signal Strength (RSS) with the Distance threshold based approach	Less Computational time and energy.	More communication overhead

1.2 Sybil Attack:

A Sybil attacker influences the network by making multiple incognito identities. This attack is used constructively with byzantine and Primary user is attacked to alter the decision making process. This alteration can lead to restricting the PUs access to the channel. In CRN each node has a legitimate identity to communicate and utilize the channel for communication. Sybil attack exploits this feature by create a large number of multiple identities and behaves like multiple geographically distinct nodes. This attacker pretends as many other users competing for communication channel [22]. Table 4 summarizes the Counter measure for Sybil attack

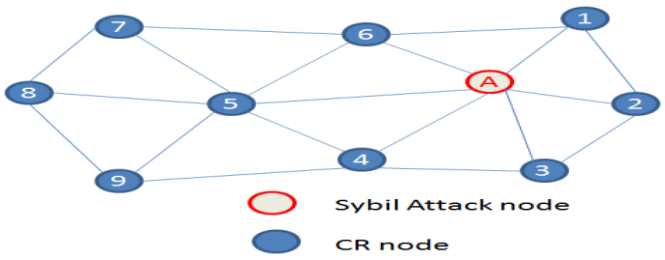

Fig.6*. Sybil Attack*

An example of such an attack is presented in Figure 6, where the Sybil node A, uses the identity of three network nodes (1, 2 and 3) to maliciously alter the nodes normal behavior.

Table 4 *summarizes the Counter measure for Sybil attack:*

Approach	Proposed Solution	Advantages	Limitations
Message Authentication and Passing (MAP) Method Udaya Suriya Raj Kumar Dhamodharan et al. [23]	This method is combination of CAM-PVM with MAP	75% detection rate from CAM-PVM and in was 90% in MAP Better throughput	More time consumption and cost effective
Hybrid MAC & MAP method Rohit Lakhanpal et at. [24]	Based on the Authentication timestamp and location of the Nodes.	Better accuracy Better throughput	More time consuming than any other method.
LIGHTWEIGHT Sybil Attack Detection P. Raghu et al. [25]	On the basis of RSS value.	It does not require any extra hardware Less expensive.	Need a bigger quantity of samples to attain accuracy.
Trust Based Sybil Detection (TBSD) Rupinder et al. [26]	This is based on manipulative trust values of adjacent nodes	Cheap More effective than the most of the existing techniques. More Accuracy	Significant performance overhead Not considered the effect of mobility of sensor nodes. Low Bandwidth utilization Low Error Detection rate
Sybil Attack Detection using Sequential Analysis (SADSA) P. Raghu Vamsi et al. [27]	Sequential Analysis	Cheaper Low processing and communication overhead. High Error Detection rate	Require to extend the method to heterogeneous and mobile WSNs.
Random Password Comparison (RPC) R. Amuthavalli et al. [28]	Delay Time, Energy, Throughput	Dynamic and Accurate Efficient	Low Positive Rate Based on neighbor analysis to identify the node

2. Taxonomy of attacks targeting the Cross layer:

Some of the attacks target multilayers of the cognitive radio networks and disturb the functionalities of the layers. In this section we are addressing Lion attack and Jellyfish attack and their detection and prevention techniques.

2.1 Lion Attack:

The Lion attack is one of PUE-based cross-layer attack targeted to reduce the throughput of Transmission Control Protocol (TCP) in the transport layer by forcing frequency handoffs [29]. The lion attack, together with the Primary User

Emulation attack, can effectively reduce the throughput of TCP. The mitigating techniques are Group key management (GKM), Freezing TCP parameters during frequency handoffs and Intrusion Detection Systems (IDSs). Table 5 summarizes the Counter measure for Lion attack.

Table 5 *summarizes the Counter measure for Lion attack:*

Approach	Proposed Solution	Advantages	Limitations
Freeze-TCP [29]	Freezing TCP parameters during frequency handoffs	Good solution to detect	Partially prevent the effects of the Lion attack but cannot stop it.
Intrusion Detection Systems (IDSs) [29]	Anomaly detection approach	Low detection latency	It detects the attack but not prevents.

1.3 Jellyfish Attacks:

Jellyfish attack is a passive attack function at the network layer but it affects the performance of the transport layer mainly on TCP Protocol. The main aim of this attack is to reduce the throughput of the TCP Protocol. There are three types of Jellyfish attack: 1) Misordering Jellyfish attack, 2) Dropping Jellyfish attack and 3) Delay variance Jellyfish attack. Jellyfish attack is difficult to detect because the attacker don't violate any of the protocol rules. Many researches are carried out to detect and prevent the Jellyfish attack [30]. In this paper we are mentioning few mitigating techniques:

- Cluster Based Technique (CBIDPT)
- Super Cluster Based Technique (SCBIDPT)
- Non-cryptography approach
- Efficient Transmission Control Protocol (E-TCP)
- Enhanced AODV routing protocols (EAODV

2. CONCLUSION

Cognitive radio is a novel and an emerging technology. Cognitive radio systems are vulnerable to security threats that affect the overall performance of a network. This is a great opportunity for the researcher to develop a secure framework for the cognitive radio networks. This paper focused attacks targeting the network layer and cross layer in the CRN and their various detection and prevention techniques were presented. In additions we discussed about limitations of each proposed techniques.

REFERENCES

[1]. El-Hajj W, Safa H, Guizani M (2011)" Survey of security issues in cognitive radio networks". Inter Technol 12(2):181–198.

[2]. J. Mitola and G. Q. Maguire, "Cognitive Radio: Making software radios more personal", IEEE personal Communications, 1989, vol. 6, no. 4, pp. 13-18..

[3]. Ameer Sameer Hamood, Sattar B. Sadkhan. "Cognitive radio network security status and challenges", Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), 2017.

[4]. John N. Soliman, Tarek Abdel Mageed, Hadia M. El-Hennawy. "Countermeasures for layered security attacks on cognitive radio networks based on modified digital signature scheme", Eighth International Conference on Intelligent Computing and Information Systems (ICICIS), 2017

[5]. Mounia Bouabdellah, Naima Kaabouch, Faissal El Bouanani, Hussain Ben-Azza. "Network layer attacks and countermeasures in cognitive radio networks: A survey", Journal of Information Security and Applications, 2018

[6]. Majid Khabbazian, Hugues Mercier, Vijay K. Bhargava. "Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks", IEEE Transactions on Wireless Communications, 2009.

[7]. Sayan Majumder, Debika Bhattacharyya. "Mitigating wormhole attack in MANET using absolute deviation statistical approach", IEEE 8th Annual Computing a Communication Workshop and Conference (CCWC), 2018

[8]. Jayashree Padmanabhan, Venkatesh Manickavasagam:Scalable and Distributed Detection Analysis on Wormhole Links in Wireless Sensor Networks for Networked Systems. IEEE Access 6: 1753-1763 (2018).

[9]. Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", IEEE 2003.

[10]. L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks". In the Proceedings of network & distributed system Security Symposium. 2004.

[11]. Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", IEEE, 2011.

[12]. Sweety goyai, harish rohil, "Securing MANET against Wormhole Attacl using Neighbour Node Analysis" IJCA volume 81, November 2013.

[13]. Lui K.-S., sChiu H.S., "DelPHI: Wormhole Detection mechanism for Adhoc Wireless Networks" Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. 16–18 January 2006.

[14]. Rana, Khurram Gulzar, Cai Yongquan, Allah Ditta, Muhammad Azeem, and Muhammad Qasim. "Circumventing sinkhole attack in ad hoc networks", International Journal of Wireless and Mobile Computing, 2015.

[15]. Krontiris, I. Dimitrou, T. Freiling, F.C. "Towards intrusion detection in wireless sensor networks". Proceedings of the 13th European Wireless Conference, Paris, France, April 2007.

[16]. S. Sharmila and G. Uma maheswari, "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms", International Conference on Process Automation, Control and Computing, (2011), pp. 1-6

[17]. D. Sheela, et al, "A non Cryptographic method of Sink hole attackDetection in Wireless Sensor Networks", IEEE-InternationalConference on Recent Trends in Information Technology, June 3-52011, pp 527-532

[18]. Chen, C., Song, M. and Hsieh, G. (2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, In Wireless Communication, Networking and

Information Security (WCNIS), IEEE Interational Conference on (pp. 711-716).
[19]. H. Khosravi, R. Azmi, and M. Sharghi "Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks" International Journal of Future Computer and Communication, Vol. 5, No. 2, April 2016
[20]. V. P. Singh, S. Jain, and J. Singhai, “Hello flood attack and its countermeasures in wireless sensor networks,” International Journal of Computer Science, vol. 7, no. 3, p. 23, 2010.
[21]. Magotra, Shikha, and Krishan Kumar "Detection of HELLO flood attack on LEACH protocol", IEEE International Advance Computing Conference (IACC), 2014.
[22]. Shehnaz T. Patel, Nital H. Mistry. "A review:Sybil attack detection techniques in WSN", 4th International Conference on Electronics and Communication Systems (ICECS), 2017
[23]. Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal.Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method the Scientific World JournalVolume 2015.
[24]. Rohit Lakhanpal, Sangeeta Sharma. "Detection & Prevention of Sybil attack in Ad hoc network using hybrid MAP & MAC technique", International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), 2016
[25]. P. Raghu Vamsi, Krishna Kant “A Light-weight Sybil Attack Detection Framework for Wireless Sensor Networks”, IEEE 2014.
[26]. Rupinder Singh, Jatinder Singh, Ravinder Singh “TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks”, IJCSNS 2016.
[27]. P. Raghu Vamsi, Krishna Kant “Sybil Attack Detection using Sequential Hypothesis Testing in Wireless Sensor Networks”, ICSPCT 2014.
[28]. R. Amuthavalli, DR. R. S. Bhuvaneshwaran “Detection and Prevention of Sybil Attack in WSN Employing Random Password Comparison Method”, JATIT 2014, Vol. 67 No.1.
[29]. Khadijeh Afhamisisi, Hadi Shahriar. Shahhoseini, Ehsan Meamari. "Defense against Lion Attack in Cognitive Radio Systems using the Markov Decision Process Approach", Frequenz, 2014
[30]. Sunil Kumar, Kamlesh Dutta, Anjani Garg."FJADA: Friendship Based JellyFish Attack Detection Algorithm for Mobile Ad Hoc Networks", Wireless Personal Communications, 2018.