ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

# Analysis of Attacks in Cognitive Radio Networks and their Counter Measures

S.Arivazhagan[1], R.Ahila Priyadharshini[2], K.Uma Haimavathi[3*]

Professor and Principal, Dept. of ECE, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India[1]

Associate professor, Dept. of ECE, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India[2]

*PG Student [Communication Systems], Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India[3]

**ABSTRACT:** Cognitive Radio Networks (CRNs) are designed to use the spectrum in an efficient manner. That is, the unlicensed users can also use the spectrum that is not used by the licensed users of that spectrum. But at the same time, they will suffer from some of the attacks also. There are different kinds of attacks possible. Some of them are Blackhole attack, Grayhole attack. Cognitive Radio Networks in the presence of these attacks will suffer a lot. The network performance will be degraded due to these attacks. Those attacks have been discussed here and the solutions are also provided to counteract them so that, the network performance can be improved and the network will be a reliable one.

**KEY WORDS:** Cognitive Radio Network, Spectrum, Blackhole, Grayhole.

## I. INTRODUCTION

Cognitive Radio Networks are the wireless networks with which the spectrum can be used in an efficient manner [1]. In normal wireless networks, the spectrum will be allotted for each different applications. The corresponding spectrum will be used by the licensed users of that spectrum. In such cases, when the spectrum is not used by the licensed users, it will be left unused. No other users can use that spectrum. Since the spectrum will not be used efficiently here. To use the spectrum efficiently, the Cognitive Radio Networks are introduced.

In CRNs, there will be licensed and unlicensed users. The licensed users will be the primary users and the unlicensed users will be the secondary users. When the primary user is using the spectrum, it will broadcast a signal to indicate all other users that it is using the spectrum [2]. So that, the secondary users will not come into the spectrum to use that. But, whenever the primary user is not using the spectrum, the secondary users will use the spectrum without causing interference to the primary users. The cognitive radios will move to different spectrums wherever the primary user is not available. Thus, to adapt to the properties of different spectrums the Cognitive Radios will have to be dynamic in nature.

## II. LITERATURE SURVEY

Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit [8] described that he MANET (Mobile Adhoc Network) is a wireless distributed network. It is formed by group of autonomous mobile nodes without any infrastructure like access points. Every node of MANET can acts as router as well as host. It has a basic characteristic of dynamic topology, it means nodes can enter and leave network any time. MANET is vulnerable to many security attacks. Black hole attack is most occurred attack in MANET and very hard to detect which is performed on network layer. Black hole attacks are classified into two types. In single black hole attack, one malicious node will change the route of source to destination and wrong path of malicious node will follow. In collaborative black hole attack one malicious node records packet at one end and send to another malicious node at other end. Black hole attacks are active attacks. In this paper, a solution for detecting black hole attack was proposed. While using EBAODV (Enhance Black hole AODV) protocol, leader nodes are used for detecting black hole nodes.

Dilraj Singh, Amardeep Singh [9] described that the self-organizing nature of the Mobile *Ad hoc* Networks (MANETs) provide a communication channel anywhere, anytime without any pre-existing network infrastructure. However, it is exposed to various vulnerabilities that may be exploited by the malicious nodes. One such malicious behavior is

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

introduced by blackhole nodes, which can be easily introduced in the network and, in turn, such nodes try to crumble the working of the network by dropping the maximum data under transmission. In this paper, a new protocol was proposed which was based on the widely used *Ad hoc* On-Demand Distance Vector (AODV) protocol, Enhanced Secure Trusted AODV (ESTA), which makes use of multiple paths along with use of trust and asymmetric cryptography to ensure data security. The results, based on NS-3 simulation, reveal that the proposed protocol was effectively able to counter the blackhole nodes in three different scenarios.

Ashok M. Kanthe, Dina Simunic, Ramjee Prasad [10] proposed a security mechanism to defend against a cooperative gray hole attack on the well known AODV routing protocol in MANETs. A gray hole is a node that selectively drops and forwards data packets after it advertises itself as having the shortest path to the destination node in response to a route request message from a source node. The proposed mechanism does not apply any cryptographic primitives on the routing messages. Instead, it protects the network by detecting and reacting to malicious activities of any node. Simulation results show that the scheme has a significantly high detection rate with moderate network traffic overhead.

## III. NEED FOR ATTACK DETECTION

Normally in wireless networks, the occurrence of attacks will be a frequent one. In addition, Cognitive Radios are having the dynamic behavior also. Due to this dynamic behavior, the possibility of attack occurrence will also be very high [3]. Thus, finding out the attacks possible in Cognitive Radio Networks and eliminating those attacks will be very important.

## IV. COGNITIVE CYCLE

Cognitive Cycle has four phases as shown in fig 1. They are Sensing, Analysis, Adaptation and Acting phases. During sensing phase, the Cognitive users will sense the spectrum to adapt to its properties [4]. During analysis phase, the channel and network characteristics like capacity, bit error rate, and delay are analysed and the analysed results will be fed to the adaptation phase. In the adaptation phase, the Cognitive Radios will configure its properties to adapt to the channel. Then it will start acting in that channel during acting phase.

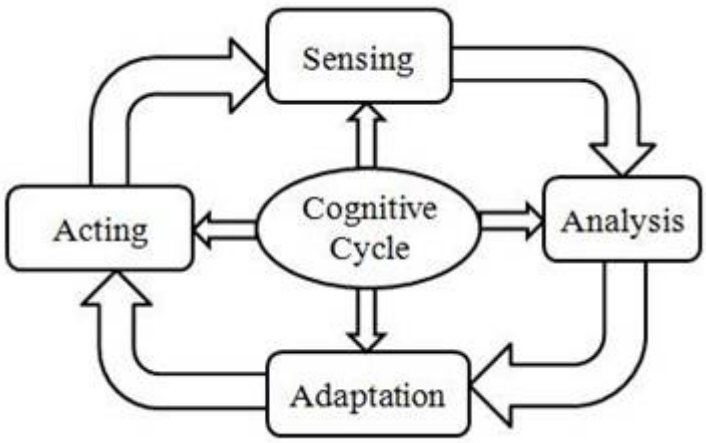


Fig. 1 Cognitive Cycle

Among these, the Sensing and Acting phases are more vulnerable to attacks. Because, during sensing phase, there may be chances that the attacker will act like a primary user and transmit a fake signal to fool other users in the network that the primary user is using the spectrum [5]. And also during actin phase, the attacker can easily jam the network traffic by sending spoofing signals. But during analyzing and adapting phases, the chances for attack to be occur will be minimum.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

## V. ATTACKS IN COGNITIVE RADIO NETWORKS

There are different kinds of attacks possible in the Cognitive Radio Network [6]. Here, two of them are mentioned and analyzed to study the performance of the network in the presence and absence of the attack [7].

## VI. BLACKHOLE ATTACK

Blackhole attack is a kind of attack in Cognitive Radio Network, which occurs at the network layer [8]. Hence, the attacks occur during routing of the handshake signals within the network.

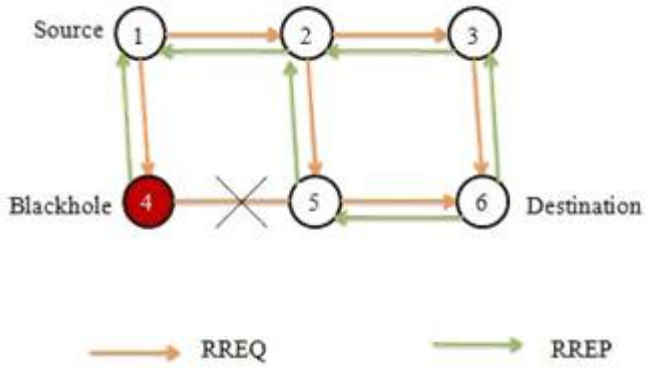


Fig. 2 Blackhole mechanism

Consider a network with 6 nodes as shown in fig 2. Here, node 1 is the source node and node 6 is the destination. The node 4 is acting as a blackhole in between the source and destination.
In order to route packets, the source initially broadcasts the route request (RREQ) signal to all the nodes in the network [9]. Then the nodes will respond its route reply with the distance between that node and the destination that is the number of hops to reach the destination.
During this period, the blackhole in the network will respond with a route reply that it is having the minimum number of hops to reach the destination. These are shown in the fig 3.

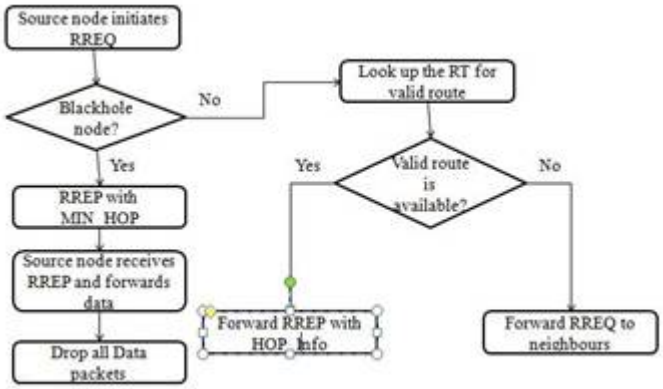


Fig 3. Blackhole algorithm

To detect a blackhole in the network, the further request (FREQ) and further response (FREP) signals are used. Once the source detected that there is no packets delivered at the destination due to the lack of acknowledgement. Then, the source will broadcast a FREQ signal to all the nodes in the network. After receiving this FREQ, all the nodes will respond with FREP which contains the route information of the node itself and also the neighbor node information. The

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

source node after receiving the FREP will cross verify the information given in the RREP. If there are any mismatches, then the source will mark the corresponding node as a Blackhole and stop transmitting packets through that node.

## VII. GRAYHOLE ATTACK

There is one more attack in the network layer known as grayhole attack [10]. This is similar to blackhole attack but the only difference is that a blackhole drops all the packets it receive and the grayhole doesnot drops all the packets. Instead, a grayhole drops the packets for a particular period of time and forwards the packets for another period of time [11]. So that, these kind of grayholes will be very hard to find.
The mechanism by which the grayhole acts is following the algorithm given in Fig 5.

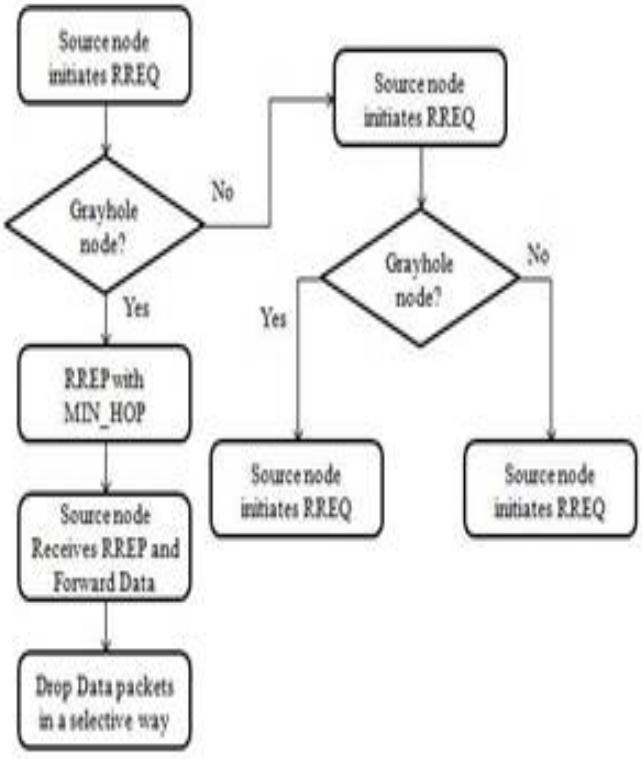


Fig 5. Grayhole mechanism

For our assumption, we are considering that the blackhole drops the packet for 2s of time and forwards the packet for another 2s. Thus it makes the detection a complex one. To detect the blackhole, the watchdog timer and pathrater are being used. , a watchdog timer starts the moment a packet is sent. Once a packet is forwarded to next hop node, the current node checks for watchdog timer duration if the packet is getting forwarded further on to the destination node or not.
The blackhole node doesn't forward packets that it receives. The watchdog timer in the node (which forwarded the packet to the blackhole node) expires. A counter is present which measures the number of times the watchdog timer expires (in other words the number of packets sent out but not forwarded by the next hop node). Once this counter's value reaches the failure threshold the next hop is marked by the current node as a blackhole node.
The pathrater validates the route. When the node is a Malicious Node and a Route Reply is processed, the function verifies the route reply in the route cache and checks for the black listed node, i.e., grayhole node. When a grayhole node is found, that route entry is deleted from the cache.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

## VIII. RESULTS

To analyze the performance of cognitive radio networks, 50 number of users will be considered and other parameters used will be given in the Table 1.

Table 1: Simulation parameters for blackhole detection

| Parameter | Description |
|---|---|
| Channel type | Wireless Channel |
| Radio Propagation Model | Two Ray Ground |
| Total number of primary and secondary users | 50 |
| Routing Protocol | AODV |
| Topological falt grid | 1000 * 1000 |

As the blackhole drops all the packets it receive, the packet delivery ratio (PDR) is an important parameter to be analyzed. This is given in Fig 4(a).

The formula used to calculate the packet delivery ratio is,

$$\text{PDR} = \frac{1}{N} \sum_{A=0}^{n} \frac{\text{Pr}*100}{Ps} \qquad \text{---------- (1)}$$


Fig. 4 (a) PDR (b) Delay (c) Throughput

The PDR decreases as the time increases and it is only about 20% of the maximum. This lack of PDR is because of the discarded packets by the blackhole.

Then, the delay is considered. As this mechanism needs additional RREQ (FREQ) and RREP (FREP), the delay for reaching a packet to reach to a destination will be very high. That is shown in Fig 4(b). The formula used to calculate end to end delay is given by,

$$\text{Delay} = \frac{1}{n} \sum_{A=0}^{n} (tr - ts) \qquad \text{---------- (2)}$$

Finally, the throughput is analyzed in the presence of attack. That is shown in Fig 4(c).

The throughput is calculated using the formula,

$$\text{Throughput} = \frac{1}{n} \sum_{A=0}^{n} \frac{(N*1024*8)}{Transmission\ time} \qquad \text{---------- (3)}$$

To analyze the performance of cognitive radio networks the parameters which have been chosen as in the case of grayhole attack as shown in Table 1. Then the packet delivery ratio, throughput and the end to end delay are analyzed here also.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 5, May 2016**

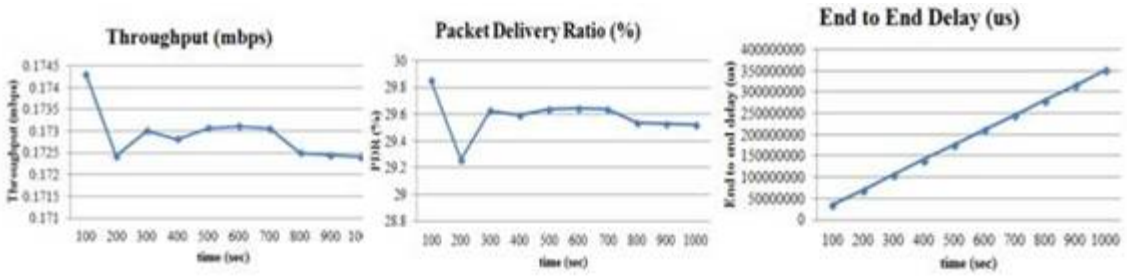


Fig. 6 (a) Throughput (b) PDR (c) Delay

From the Figures 6(a), 6(b) and 6(c), it is clear that the grayhole attack created a high impact in the cognitive radio networks. But when compared to blackhole, grayhole does not affects the performance of the network that much.

## IX. CONCLUSION

Thus, the cognitive radio networks, due to their dynamic property will suffer a lot by different kinds of attacks. Finding out these kinds of attacks and eradicating those attacks will be a very important. Among the two kinds of attacks simulated, the blackhole made a very much impact in the network. Here, the attack mechanisms were analyzed and the countermeasures for eradicating those attacks are also given. So that, the network performance is improved by providing perfect countermeasures.

## REFERENCES

[1] Ying-Chang Liang, Kwang-Cheng Chen, Geoffrey Ye Li, Petri Mähönen, "Cognitive Radio Networking and Communications: An Overview", IEEE Transactions on Vehicular Technology, Vol. 60, No. 7, September 2011.
[2] Konstantinos Pelechrinis, Prashant Krishnamurthy, Martin Weiss, Taieb Znati, "Cognitive Radio Networks: Realistic or Not?", ACM SIGCOMM Computer Communication Review, Volume 43, Number 2, April 2013.
[3] Suchismita Bhattacharjee, Roshni Rajkumari, Ningrinla Marchang, "Cognitive Radio Networks Security Threats and Attacks: A Review", International Journal of Computer Applications (0975 – 8887), International Conference on Information and Communication Technologies (ICICT-2014).
[4] Rajesh K. Sharma, Danda B. Rawat, "Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey", IEEE Communication Surveys & Tutorials, Vol. 17, No. 2, Second Quarter 2015.
[5] Alexandros G. Fragkiadakis, Elias Z. Tragos, Ioannis G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks", IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, First Quarter 2013.
[6] M.Padmadas, Dr.N.Krishnan, V.Nellai Nayaki, "Analysis of Attacks in Cognitive Radio Networks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 8, August 2015.
[7] Dr. Anubhuti Khare, Manish Saxena, Roshan Singh Thakur, Khyati Chourasia. Attacks & Preventions of Cognitive Radio Network-A Survey. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.
[8] Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit. A Novel Approach for Detection of Blackhole Attacks. IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 69-74.
[9] Dilraj Singh, Amardeep Singh. Enhanced Secure Trusted AODV (ESTA) Protocol to Mitigate Blackhole Attack in Mobile Ad Hoc Networks. Future Internet 2015, 7.
[10] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad. A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks. International Journal of Computer Applications (0975 – 8887), Volume 53– No.16, September 2012.
[11] Sandeep Kumar, Mrs. Sangeeta, Pramod Kumar Soni. Evaluation of Gray Hole Attack in Mobile Ad-hoc Network and proposed Solution. International Journal of Advanced Research in Computer Science and Software Engineering 4(11), November - 2014, pp. 535-541.