ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Analysis of Wormhole Attack with AODV Routing Protocol in MANETs using NS3.26 Network Simulator

Neelam Janak Kumar Patel[1], Dr. Khushboo Tripathi[2]

Ph.D. Research Scholar, Dept. of CSE, ASET, Amity University, Haryana, India[1]

Assistant Professor, Dept. of CSE, ASET, Amity University, Haryana, India[2]

ABSTRACT: As MANETs use wireless medium for communication, these are vulnerable to many kind of security attacks like Blackhole attacks, Wormhole attacks, Sybil attacks etc. Security is an essential requirement in MANETs. A proper security solution is needed for networks to protect both route and data packet delivery operation in the network layer. The malicious node in the network act as a normal node, so there is a need of security solution to prevent from various attacks. This paper presents analysis of wormhole attacks in MANETs using AODV routing protocol. Use 25 nodes in Mobile ad hoc network with 0 attack, 1 attack, 3 attacks and 5 numbers of wormhole attacks nodes treated with reactive protocol AODV. The performance results are analyzed based on Throughput, Packet loss and Delay time with same simulation time for different numbers of malicious nodes for wormhole attacks using NS3.26 network simulator on Ubuntu 14.04.4 LTS version platform.

KEYWORDS: AODV; MANETs; DSDV; DSR; ZRP,WORMHOLE ATTACK

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is used all around the world, because it has ability to communicate with each other without the use of any pre-established network infrastructure. It is decentralized, all network and routing activities are handled by nodes. Wireless nodes are free to move and cause dynamic topology. Due to the limitations of the medium, communications can easily be disturbed; vulnerable to much kind of attacks. Here we focus on attacks against the routing protocol in ad hoc networks. Routing is the fundamental operation in MANETs that facilitates the establishment of communication links between nodes and the packet delivery [1]. These attacks may have the aim of modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. An attack may also aim at blocking the establishment of the network, making genuine nodes store incorrect routes, and more generally at disturbing the network topology.

Attacks are classified in to two categories, Static attacks and Mobile attacks. Identity Attack (e.g. Sybil attack, Clone attacks), routing attack (e.g. sinkhole attack, false routing attack, selective forwarding attack) and network Intrusion Attack are the static attacks [2]. There are two types of mobiles attacks that are Hardware attacks and Software attacks. Hardware attacks are two types which are internal attacks (e.g. Extensive and Exclusive attacks) and external attacks (e.g. Jamming and Collision attacks).

Wormhole attack is one of the severe attacks in Mobile Ad hoc network [3] detecting the wormhole attack using Reactive routing protocol, Ad hoc On-Demand Distance Vector (AODV), this research paper presents analysis of wormhole attacks using AODV in NS3.26 network simulator on Ubuntu 14.04.4 LTS.

II. AODV

The Ad hoc on-Demand Distance Vector (AODV) routing protocol is estimated for use by mobile nodes in an ad hoc network. AODV algorithm enables dynamic, self-starting, multi hop routing between contributing mobile nodes desiring to established and maintain an ad hoc network [12]. AODV is on demand routing protocol has obtain routes

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

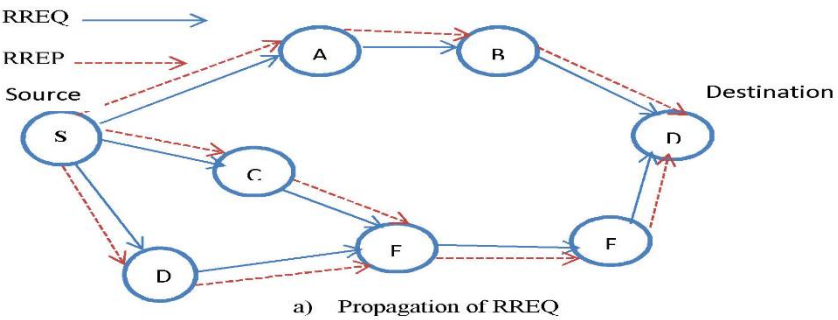
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

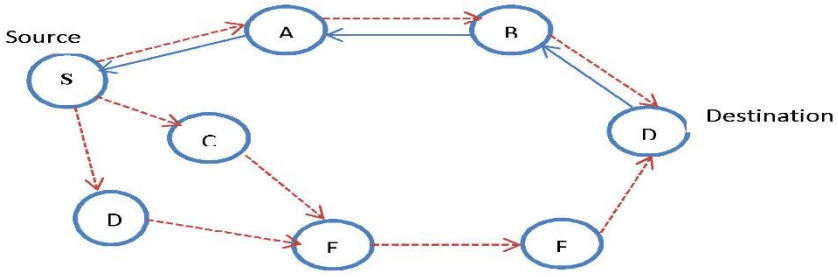
Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication [1, 9].



a) Propagation of RREQ



b) Propagation of RREP to the source

Fig 1 AODV route discovery

AODV routing table maintains by following information: [1, 9]

- Destination IP address
- Destination sequence number
- Hop count
- Next hop
- lifetime (route expiration time)

Basic message set in AODV includes: [1, 9, 12]

- Hello- For link status
- RREQ- Route Request
- RREP- Route Reply
- RERR- Route Error

WORMHOLE ATTACK

The wormhole attack is most severe attacks encounter mobile ad hoc network, it can overcome the authenticity and confidentiality communication, and this shows the seriousness of this attack. One of the attackers captures the traffic at one point and tunnels them to another point to other attacker and further in the network [11]. Recording traffic from one region of the network and replaying it in a different region. This influences the neighbour nodes of these two end points that these two distant points at either end of the tunnel are very close to each other. If one end of the tunnel is at near to the base station, the wormhole tunnel is at near to the base station, the wormhole tunnel can attract substantial amount of data traffic to annoy the routing and operational functionality of MANETs [2]. In this case, the attack is like sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station.

Each ROUTE REQUEST (RREQ) packet is tunnelled to the destination target node of the REQUEST for the application of wormhole attack [13]. Normal routing protocol process is to be followed when the destination node's neighbour received this REQUEST packet which will rebroadcast that copy of REQUEST and then recklessness all other received ROUTE REQUEST packets activated from this same Route Discovery. Any routes other than the routes which are being explored can be prohibited by

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

this attack. In addition to that the attack can even prevent routes more than two hops long from being visible, if the attacker is near the originator of route investigation [17].

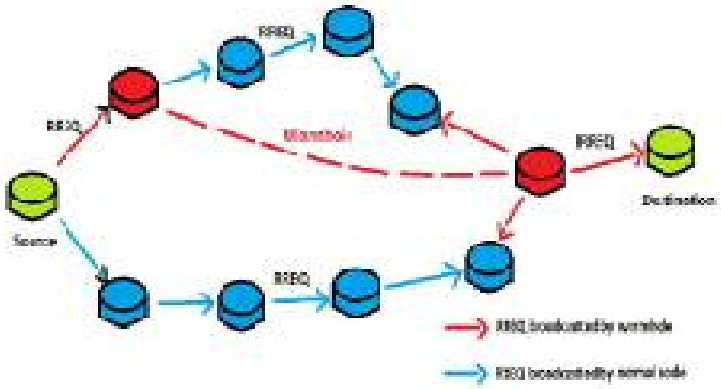


Figure 2: Wormhole Scenario [17]

As shown in Figure 2, malicious node that is red in color will be announcement its RREQ to its neighbour nodes which is originally broadcasted to perform a wormhole attack. Destination node will receive the RREQ request so it will follow a normal routing process and remove all other received ROUTE RQUEST packets. The malicious node will create a link to another malicious node which is the neighbour of the source node which is dotted in fig 2 known as wormhole tunnel.

The tunnel in turn to be a shortest path to reach the destination as it may have less hop count compare to normal routes. Various kind of attack such as DOS attack, Eavesdropping, and fabrication can be performing with the use of this opportunity. Wormhole attack can disturb the entire routing system in MANET.

The attacker assists useful services more capably for connecting the network, if the attacker achieves this tunnelling reliably and honestly and no loss is done. The attacker can still be launched even if confidentiality and authenticity is provided over the communication and even if the intruder has no cryptographic keys [17].

III. SIMULATION ENVIRONMENT AND RESULTS

The simulation results are shown for parameters like Packet loss, Throughput and average end to end delay at destination by comparing normal AODV and wormhole affected AODV in a network. Initially the readings of normal AODV are noted based on above described parameters for 25 nodes. Then the wormhole nodes are added (e.g. 1 attack, 3 attacks and 5 attacks) in Normal conditions and results are noted again. The mobile ad hoc network environment is formed using network simulator NS3.26. The following table indicates the simulation parameters.

Table 1 simulation Parameters

Simulator	NS-3(Ver. 3.26)
Routing protocol	AODV
Number of wormhole nodes	0,1,3 and 5 nodes
Node speed	10m/s
Number of nodes	25
Simulation time	100s
Mobility model	Random way point

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

To evaluate the parameters of the wormhole attack with AODV routing protocol, we compare on x axis total simulation time in sec with y axis number of packet loss, Throughput and Average End to End delay in case of normal AODV, one wormhole attack, three wormhole attacks and five wormhole attacks.
Three simulation scenarios are considered.

A. Total simulation time in sec in case of No attack, one attack, three attacks and five wormhole attacks Vs. Number of Packet loss scenario.
B. Total simulation time in sec in case of No attack, one attack, three attacks and five wormhole attacks Vs. Throughput scenario
C. Total simulation time in sec in case of No attack, one attack, three attacks and five wormhole attack Vs Average End-to-End delay for each flow(ns) scenario

A. Scenario 1

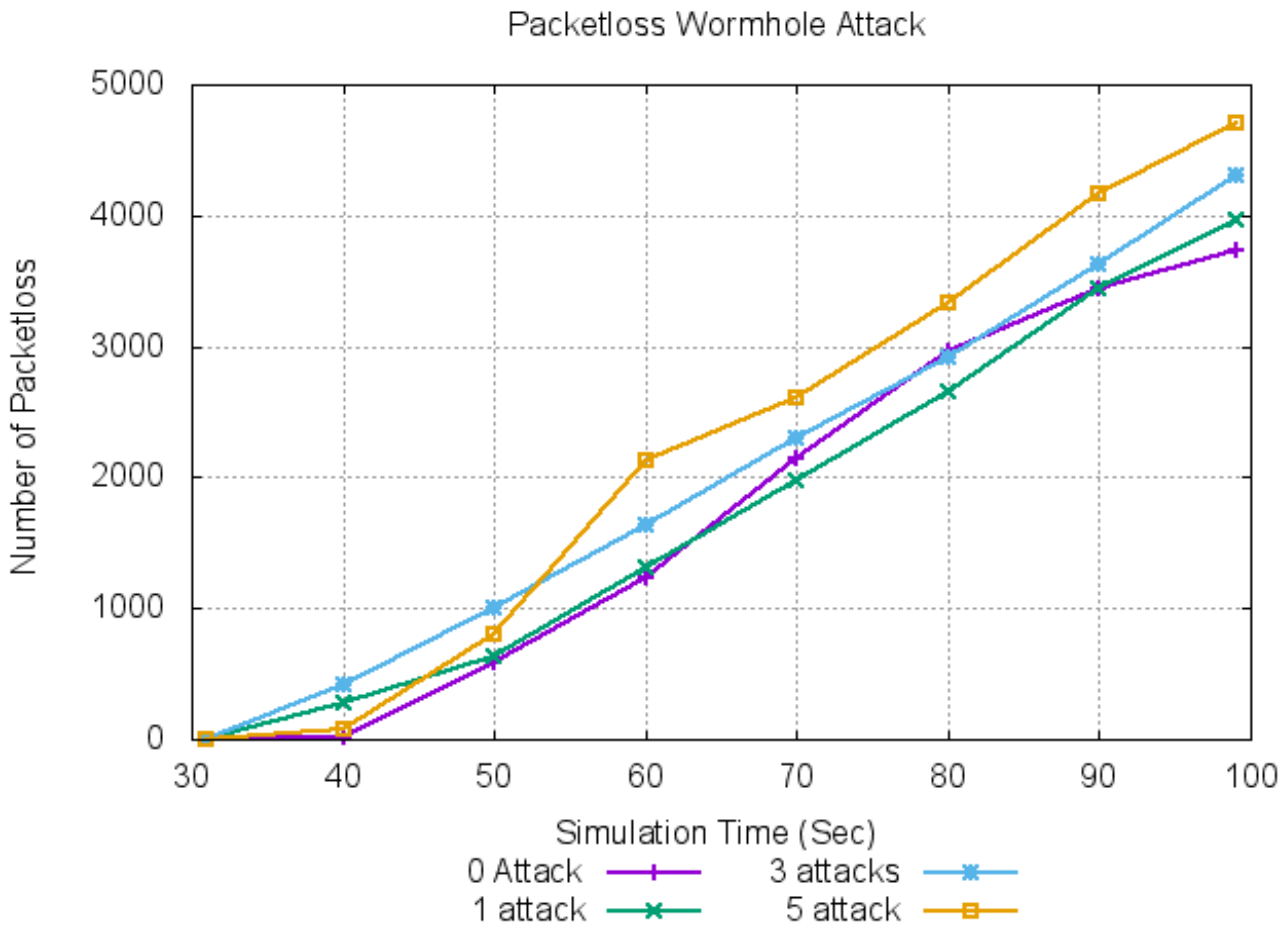


Figure 3: Simulation time Vs. Number of packet loss in case of No attack, 1 attack, 3 attacks and 5 attacks.

Figure 3 shows that the number of packet loss are plotted against simulation time starting from 30 sec to 100 sec. during that time the number of packet loss due to various reasons. The lower value of the packet lost means the better performance of the protocol. In this scenario packet loss is minimum in case of 0 wormhole attack.

Packet lost = No of packet send - No of packet received.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

B. Scenario 2

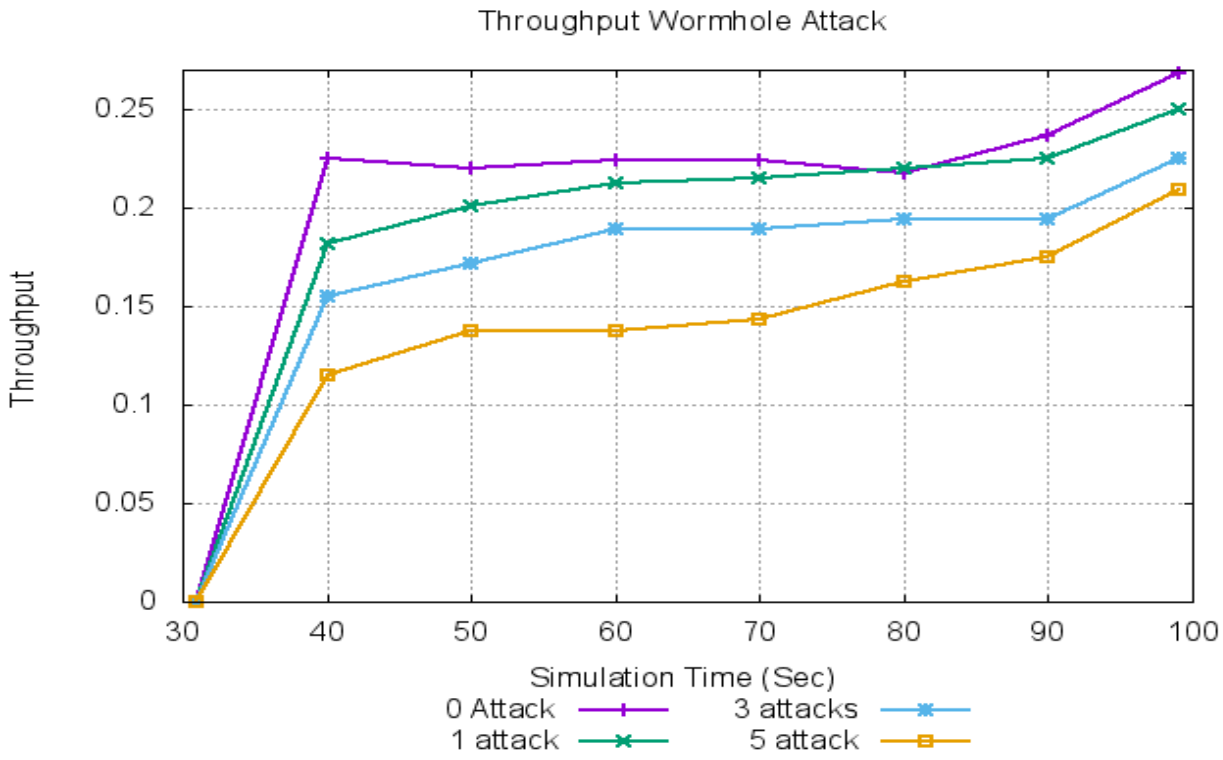


Figure 4: Simulation time Vs. Throughput in case of No attack, 1 attack, 3 attacks and 5 attacks.

Figure 4 shows that the values of average throughput are plotted against simulation time in case of No attack, 1attack, 3 attacks and 5 attacks. In this scenario, the throughput is high then other in case of 0 wormhole attacks. The throughput is the measure of how fast we can send data through the network. It is the measurement of number of packets that are transmitted through the network in a unit of time. It is necessary to have a network with high throughput.

$$\text{Throughput} = \Sigma \text{ PR} \quad [1]$$
$$\Sigma t_{st} - \Sigma t_{sp}$$

Where, PR – Received Packet Size,

t_{st}-Start Time,

t_{sp}- Stop Time.

Unit – Kbps (Kilobits per second)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

C. Scenario 3

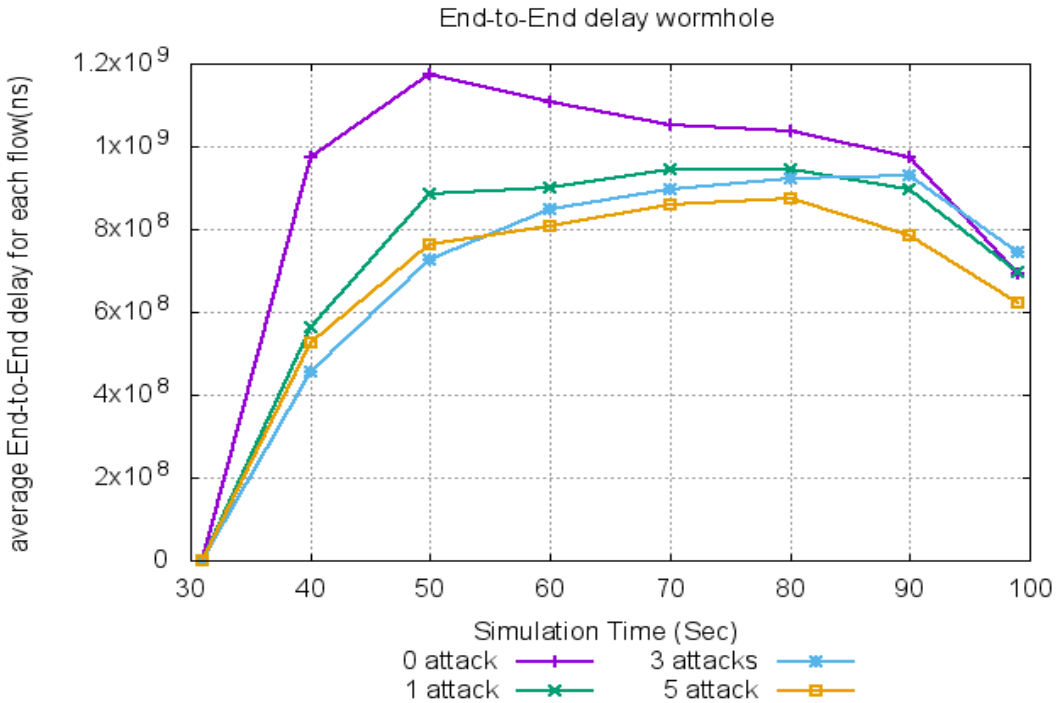


Figure 5: Simulation time Vs. End-to-End delay in case of No attack, 1 attack, 3 attacks and 5 attacks.

Figure 5 shows that average end-to-end delay for each flow against simulation time. End-to-End Delay refers to the time taken for a packet to be transmitted across a network from source to destination. In this scenario, we observe that the end-to-end delay is less in the presence of 5 wormhole attack in network as compared to other, because of 5 wormhole attacks are present in network at that time packet loss is maximum so delay time is less as compare to other from starting 30 sec to 100 sec.

Average End-to-End Delay=$\Sigma t_{PR} - \Sigma t_{PS}$ [1]

Where, t_{PR} – Packet Receive Time,

t_{PS} – Packet Send Time

Unit – Milli Seconds (ms).

IV. CONCLUSION

Simulation results obtained using NS-3.26 network simulator on Ubuntu 14.04.4 LTS version platform. The value of the parameters such as Packet loss are increases with the simulation time in case of 0 wormhole attack, 1 wormhole attack, 3 wormhole attacks and 5 wormhole attacks in networks respectively. The value of the parameters such as Throughput are decreases with the simulation time in case of 0 wormhole attack, 1 wormhole attack, 3 wormhole attacks and 5 wormhole attacks in networks respectively. According to the results we found that in case of 5 attacks the packet loss is high compare to other attacks. When the packet loss is high at that time the Throughput is lower.

REFERENCES

1. Amandeep Kaur and Kuldeep Singh, " Performance Analysis of AODV Protocol with TCP/FTP Traffic and Improved AODV Protocol with UDP/CBR Traffic for Optimizing Routing and QoSin MANET," International Journal of Advanced Research in Computer Science, Volume 8, No. 3, March – April 2017.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

2. Parmar Amish and V. B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol," Procedia Computer Science 79 (2016) 700 – 707.
3. Sarika S, Pravin A et al., "Security Issues In Mobile Ad Hoc Networks," Procedia Computer Science 92 (2016) 329 – 335.
4. Madhura Mahajan, Dr. KTV Reddy et al., "Design and Simulation of a Blacklisting Technique for Detection of Hello flood Attack on LEACH Protocol", Procedia Computer Science 79 (2016) 675 – 682.
5. Jianwei Niu, Long Cheng, YuGu, Lei Shu, and Sajal K. Das," *R*3E: Reliable Reactive Routing Enhancement for Wireless Sensor Networks," IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 10, NO. 1, pp. 784-794, FEBRUARY 2014.
6. Charalambos Sergiou, Pavlos Antoniou,and Vasos Vassiliou, "A Comprehensive Survey of Congestion Control Protocols in Wireless Sensor Networks," IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, pp. 1839-1858, FOURTH QUARTER 2014.
7. Rajesh K. Sharma and Danda B. Rawat, "Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey," IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 2, pp. 1023-1042, SECOND QUARTER 2015.
8. Hamid Al-Hamadi and Ing-Ray Chen, "Adaptive Network Defence Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 12, NO. 3, pp. 451-465, SEPTEMBER 2015.
9. Tarek M. Mahmoud, Abdelmgeid A. Aly et al., "A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs", International Journal of Computer Applications (0975 – 8887) ,Volume 109 – No. 6, January 2015.
10. Aboli Arun Anasane, Prof. Rachana Anil Satao, "A Survey on various Multipath Routing protocols in Wireless Sensor Networks," 7th International Conference on Communication, Computing and Virtualization 2016, Elsevier, Procedia Computer Science 79 (2016) 610 – 615.
11. Issa Khalil, Saurabh Bagchi et al., "UNMASK: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks," Elsevier, Ad Hoc Networks 8 (2010) 148–164.
12. Stefan K. Stafrace and Nick Antonopoulos, "Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks," Elsevier, Computer Communications 33 (2010) 619–638.
13. H. Shafiei and A. Khonsari et al., "Detection and mitigation of sinkhole attacks in wireless sensor networks," Journal of Computer and System Sciences 80 (2014) 644–653.
14. Eliana Stavrou and Andreas Pitsillides, "A survey on secure multipath routing protocols in WSNs," Elsevier, Computer Networks 54 (2010) 2215–2238.
15. Miao Xie, Song Han et al., "Anomaly detection in wireless sensor networks: A survey," Elsevier, Journal of Network and Computer Applications 34 (2011) 1302–1325.
16. Ashfaq Ahmada, Muhammad Babar Rasheeda et al., "Hop Adjusted Multi-chain Routing for Energy Efficiency in Wireless Sensor Networks," Procedia Computer Science 37 (2014) 236 – 243.
17. Ashka Shastri and Jignesh Joshi., "A Wormhole Attack in Mobile Ad-hoc Network: Detection and Prevention," *ICTCS '16*, March 04-05, 2016, Udaipur, India, 2016 ACM. ISBN 978-1-4503-3962-9/16/03…$15.00, DOI: http://dx.doi.org/10.1145/2905055.2905237.
18. Neelam Janak kumar Patel and Dr. Khushboo Tripathi, "Detection & Prevention Techniques of Sinkhole Attack in Mobile Adhoc Network: A Survey," *International Journal of Latest Research in Engineering and Technology (IJLRET) ISSN: 2454-5031 www.ijlret.com,Volume 2 Issue 4,PP 50-54, April 2016.*
19. Neelam Janak kumar Patel and Dr. Khushboo Tripathi, "Sinkhole Attack Detection and Prevention inWSN & Improving the Performance of AODV Protocol," International Journal of Innovative Research in Computerand Communication Eng. (An ISO 3297: 2007 Certified Organization), ISSN(Online): 2320-9801 ISSN (Print): 2320-9798,Vol. 4, Issue 5, pp. 9660-9669, May 2016.
20. Neelam Janak kumar Patel and Dr. Khushboo Tripathi, "Detection & Prevention Techniques of Sybil Attack & its Analysis in Mobile Adhoc Network," International Journal of Innovative Research in Science, Engineering and Technology(An ISO 3297: 2007 Certified Organization), ISSN(Online): 2319-8753 ISSN (Print): 2347-6710, Vol. 5, Issue 7, pp. 1111-1121, July 2016.
21. Neelam Janak Kumar Patel, Dr. Khushboo Tripathi, "Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169, Volume: 5 Issue: 5 194 – 205, May 2017.