Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26

Neelam Janak Kumar Patel[1], Dr. Khushboo Tripathi[2]
[1]Ph.D. Research Scholar, Dept. of CSE, ASET, Amity University Haryana, India
[2]Assistant Professor, Dept. of CSE, ASET, Amity University Haryana, India

Abstract: This research paper presentsanalysis of Black hole attacks in Mobile Adhoc network (MANET) routing protocol Ad Hoc On-Demand Distance Vector (AODV). Weuse 25 nodes in wireless sensor network with no attack, one attack, three attacks and five numbers of attacks nodes treated with reactive routing protocol AODV. A Simulations have been conducted in ns-3.26, which is the latest version of ns3 network simulator on Ubuntu 16.04.2 LTS version platform. The performance resultsare analyzed based on Throughput, Packet loss and Delay time with same simulation time for different numbers of malicious nodes in black hole attacks on MANET's.

Key words*: AODV; MANET; DSDV; OLSR; DSR; ZRP*

*****

1. INTRODUCTION

Black hole attacks are the main destructive attack in MANET. They destroy all the structure of network. A black hole attack on a MANET refers to an attack by a malicious node, which forcibly acquires the route from a source to a destination by the falsification of sequence number and hop count of the routing message. A selective black hole is a node that can optionally and alternately perform a black hole attack or perform as a normal node. A wireless mobile ad hoc network (MANET) consistsof so many tiny mobile nodes which are connected through wireless medium.Sensor nodes are used to monitor record and notify specific condition like temperature, humidity, wind, pressure any many more at various locations. Wireless sensor networks are becoming a cost effective. It protects confidentiality, integrity and availability of communications. It is used as a large range of applications from civilian to military purposes. Wireless medium is the challenging factor because it is less secure. Mobility of nodes and its large scalability make the network more complex. Bandwidth, memory, computational complexity, energy is the major concern for designing the securities mechanisms.

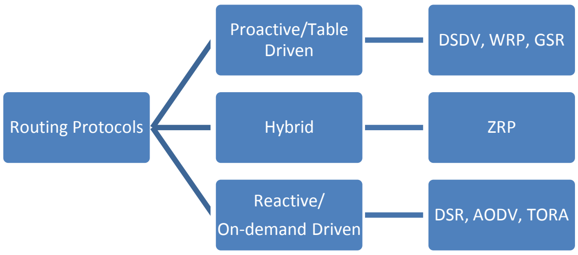


Figure1: Wireless Ad hoc Routing protocols

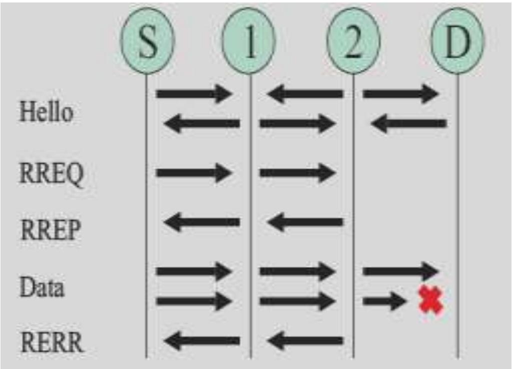


Figure 2: AODV Control messages

Routing protocols are mainly categorized into proactive routing protocols and reactive routing protocols as shown in Figure.1.In a proactive routing protocol, every node proactively searchesfor routes to other nodes and routing table with all paths maintained at each node periodically,to ensure that the information in the routing table isup-to-date and correct, such as DSDV (Destination Sequence DistanceVector) [1] and OLSR (Optimized Link State Routing Protocol) [2]. In a reactive routing protocol,a route is searched and established only when two nodes intendto transfer data;Discovers route when required and therefore, it is also called an on-demand routingprotocol, such as AODV (Ad hoc On-Demand Distance Vector) [3] or DSR (Dynamic Source Routing) [4]. A source node usually broadcasts a route request message to the entire network bymeans of flooding, to search for and establish a route tothe destination node. The AODV [3] [4-10] is the most popular routingprotocol; it minimizes the number of broadcasts by creating routes on-demand. It is a reactive or demand-driven protocol which calculates the route when required and caches it for further use. Routing table only maintains next hop for the destination rather than complete route.Freshness of route is maintained by sequence numbers. In a hybrid protocol, it is a combination of proactive & reactive protocols, such as ZRP (Zone Routing Protocol) [4-5].

2. BACKGROUND AND PREVIOUS WORK

MANETs are normally infrastructure-less and independent networks [2] where a set of mobile nodes are connected by wirelessadhoc links. The design of routing protocols for MANETs is complex because of several constraints. These routing protocol aimto provide paths that are not only optimum in terms of some standards (minimum distance, maximum bandwidth, and shortest delay) but also in satisfying some constraints, for example, the limited power of mobile nodes and the limited capacity of wirelesslinks. The most widely used MANET[11] [12] [13] routing protocols are AODV (Ad hoc On-Demand Distance Vector) [4-10], OLSR (Optimized Link StateRouting) [5], and DSR (Dynamic Source Routing) [3]. The work in this paper focuses to explore the securityvulnerabilities related to AODV, such as the impact of Black hole attacks.

2.1.AODV

Reactive protocols seek to set up routes on-demand. If a node wants to initiate communication with a node to which it has no route, the routing protocol will try to establish such a route.AODV defines three types of control messages for route maintenance shown in figure 2.

RREQ - A route request message is transmitted by a node requiring a route to a node.

As an optimization AODV uses an expanding ring technique when flooding hello messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received.

RREP - A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a “precursor list”, containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

2.2. BLACK HOLE ATTACK ON AODV PROTOCOL

In wireless sensor network, blackhole refer to places in the network were incoming packets are silently discarded or dropped without informing the source that data did not reach its destination.There are more than one black hole nodes exists in the network at different places todropping the data packets, shown in figure 3. In an AODV routing protocol, node S would broadcast a Route Request (RREQ) packet to search for destination node D; the normal intermediate nodes would receive and continuously broadcast the RREQ, rather than the black hole node. The black hole node would directly reply through a RREP with an extremely large sequence number and hop count of 1 to source node S. when receiving RREQs from normal nodes, the destination node D would also select a route with a minimal hop count, and then return a Route Reply (RREP) packet. According to the AODV design, a source node would select the latest (largest sequence number) and shortest route (minimal hop count)to send data packets upon receipt of several RREPs packets. Thus, a route via a black hole node would be selected by node S. The black hole node will then eavesdrop, or directly drop the received data packets.

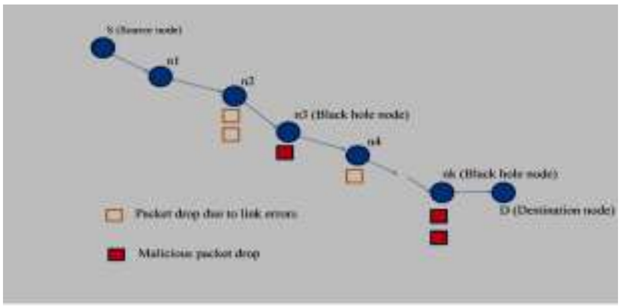


Figure 3: Multiple Black Hole Nodes

2.3 NS-3.26

In this research, the simulation tool used for analysis is NS-3.26 which is the latest version of ns3 network simulator. This simulator is highly preferred for academic networking research since it demonstrated the best overall performance.The ns-3 has derived AODV as a sub-class of the Ipv4Routingmain class, hence AODV inherits all the functions which are part of the Ipv4 routing and plus the extra methods and functionswhich are specific to the AODV protocol.

3. SIMULATION AND SCENARIOS

The experiments were setup to understand the severity of black hole attacks on MANETnodes running AODVprotocol [14]. The simulation environment uses Wireless ad hoc network [11-17], which consist of 25 nodes.

3.1 Performance Parameters

We recorded three parameters [11-17] to analyze the performance of AODV nodes under variable rate black hole attack.

Throughput: This is defined as the total amount of data (b_i) that the destination receives them from the source divided by the time (t_i) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput for n application traffics, which is denoted by T, is obtained as:

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i} \qquad (1)$$

Average End-to-End Delay: This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is d_i, and the number of packets received by the destination node is $pktd_i$. The average end-to-end delay for n application traffics, which is denoted by E, is obtained as:

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pktd_i} \qquad (2)$$

Packet Loss: The packets are loss when it is not able to find the valid route to deliver the packets.

4. RESULTS

To clearly analyse and understand the attacks we have implemented the following are the tables:

· Table 1- Variable parameters for simulation

· Table 2-Analysing Black Hole Attack (0, 1, 3, 5): Simulation Time (Sec) Vs. Number of Packet loss

· Table 3- Analysing Black Hole Attack (0,1,3,5): Simulation Time (Sec) Vs. Throughput

· Table 4- Analysing Black Hole Attack (0, 1, 3, 5): Simulation Time (Sec) Vs. Average End-to-End delay (ns)

-Table 5- Analysing Normal AODV and Black Hole AODV (0 Attack)

-Table 6- Analysing Normal AODV and Black Hole AODV (1 Attack)

-Table 7- Analysing Normal AODV and Black Hole AODV (3 Attacks)

-Table 8- Analysing Normal AODV and Black Hole AODV (5 Attacks)

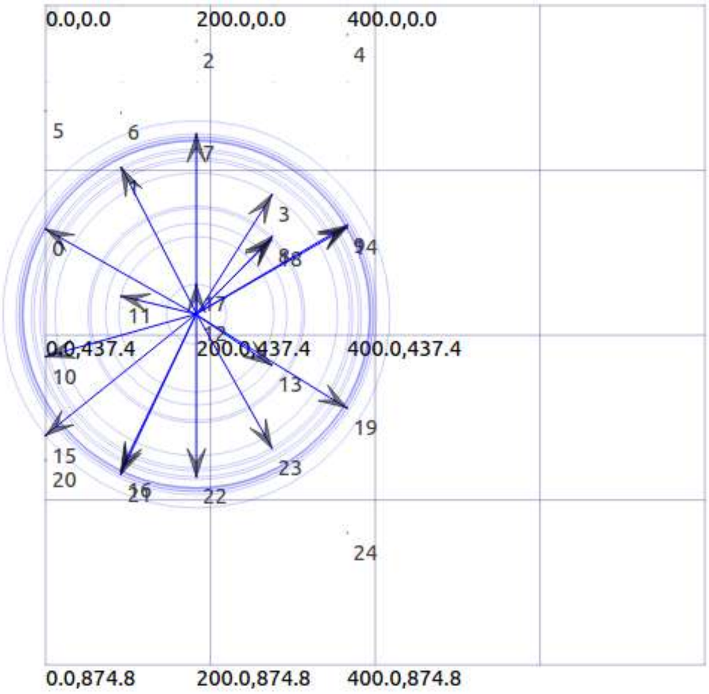
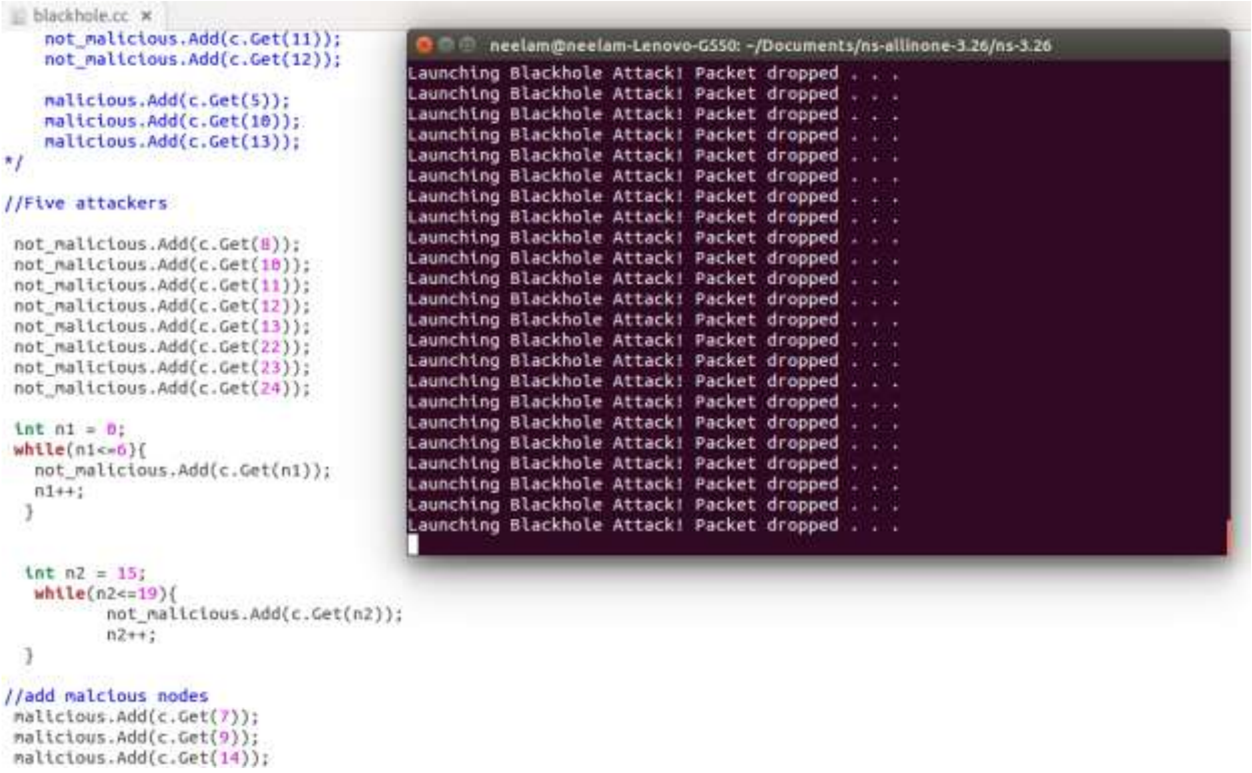


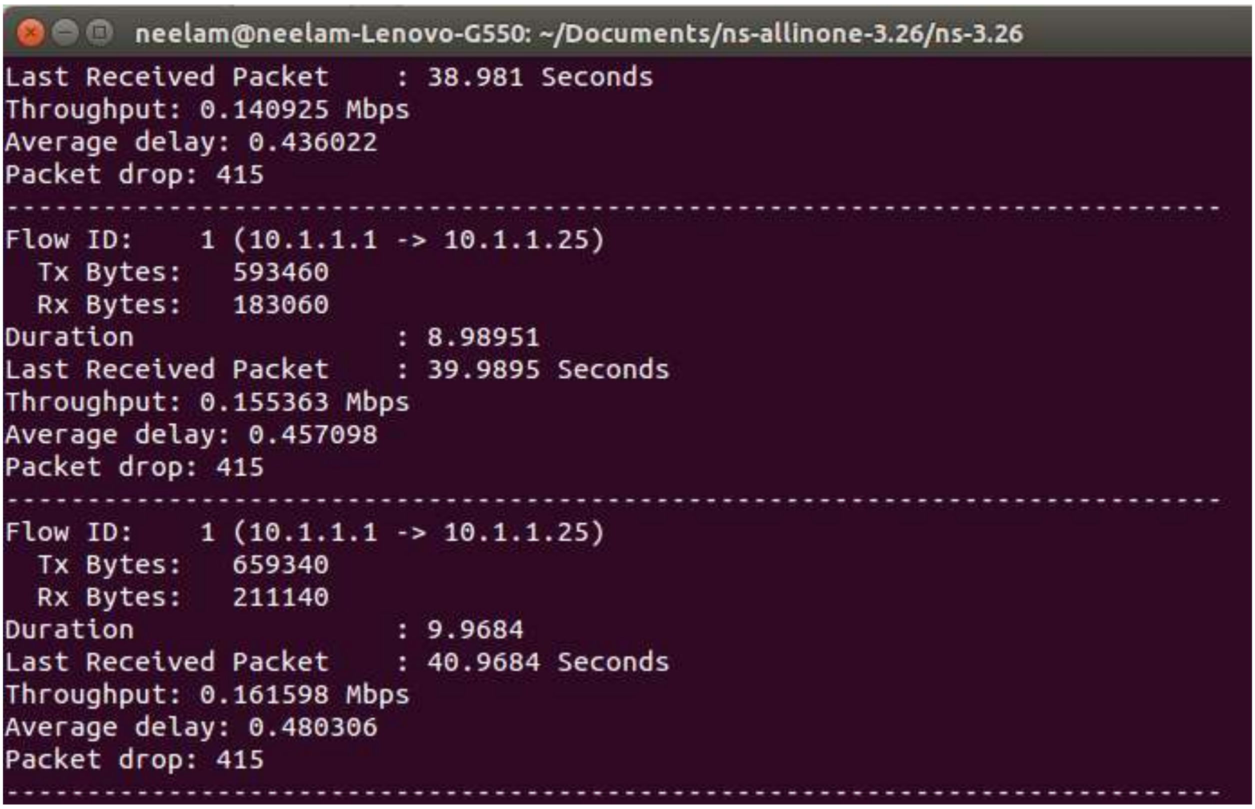
Figure 4: Black hole attack in Cartesian representation for5 black holes


blackhole.cc
neelam@neelam-Lenovo-G550: ~/Documents/ns-allinone-3.26/ns-3.26

```
    not_malicious.Add(c.Get(11));
    not_malicious.Add(c.Get(12));

    malicious.Add(c.Get(5));
    malicious.Add(c.Get(10));
    malicious.Add(c.Get(13));
*/

//Five attackers

 not_malicious.Add(c.Get(8));
 not_malicious.Add(c.Get(10));
 not_malicious.Add(c.Get(11));
 not_malicious.Add(c.Get(12));
 not_malicious.Add(c.Get(13));
 not_malicious.Add(c.Get(22));
 not_malicious.Add(c.Get(23));
 not_malicious.Add(c.Get(24));

 int n1 = 0;
 while(n1<=6){
   not_malicious.Add(c.Get(n1));
   n1++;
  }


  int n2 = 15;
   while(n2<=19){
          not_malicious.Add(c.Get(n2));
          n2++;
  }

//add malcious nodes
 malicious.Add(c.Get(7));
 malicious.Add(c.Get(9));
 malicious.Add(c.Get(14));
```

```
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
Launching Blackhole Attack! Packet dropped . . .
```

Figure 5: Launchingblack hole Attack


neelam@neelam-Lenovo-G550: ~/Documents/ns-allinone-3.26/ns-3.26

```
Last Received Packet    : 38.981 Seconds
Throughput: 0.140925 Mbps
Average delay: 0.436022
Packet drop: 415
---------------------------------------------------------------------------
Flow ID:     1 (10.1.1.1 -> 10.1.1.25)
  Tx Bytes:    593460
  Rx Bytes:    183060
Duration                : 8.98951
Last Received Packet    : 39.9895 Seconds
Throughput: 0.155363 Mbps
Average delay: 0.457098
Packet drop: 415
---------------------------------------------------------------------------
Flow ID:     1 (10.1.1.1 -> 10.1.1.25)
  Tx Bytes:    659340
  Rx Bytes:    211140
Duration                : 9.9684
Last Received Packet    : 40.9684 Seconds
Throughput: 0.161598 Mbps
Average delay: 0.480306
Packet drop: 415
---------------------------------------------------------------------------
```

Figure 6: 5 Attacks black hole –Normal AODV Running Result

Table 1. Variable parameters for simulation

Property	Values
Routing Protocol	Normal AODV, AODV with Black Hole
Number of black holes	0,1,3,5
Number of nodes	25

Table 2. Black Hole Attack: Simulation Time (Sec) Vs. Number of Packet loss

Simulation Time (Sec)	0 Black Hole Attack	1 Black Hole Attack	3 Black Hole Attacks	5 Black Hole Attacks
31	0	0	0	0
40	70	823	1095	959
50	797	1668	2319	1947
60	2122	2737	3540	3101
70	2610	3966	4761	4751
80	3334	4915	5981	5981
90	4168	5654	7202	7202
99	4707	5925	7333	7391

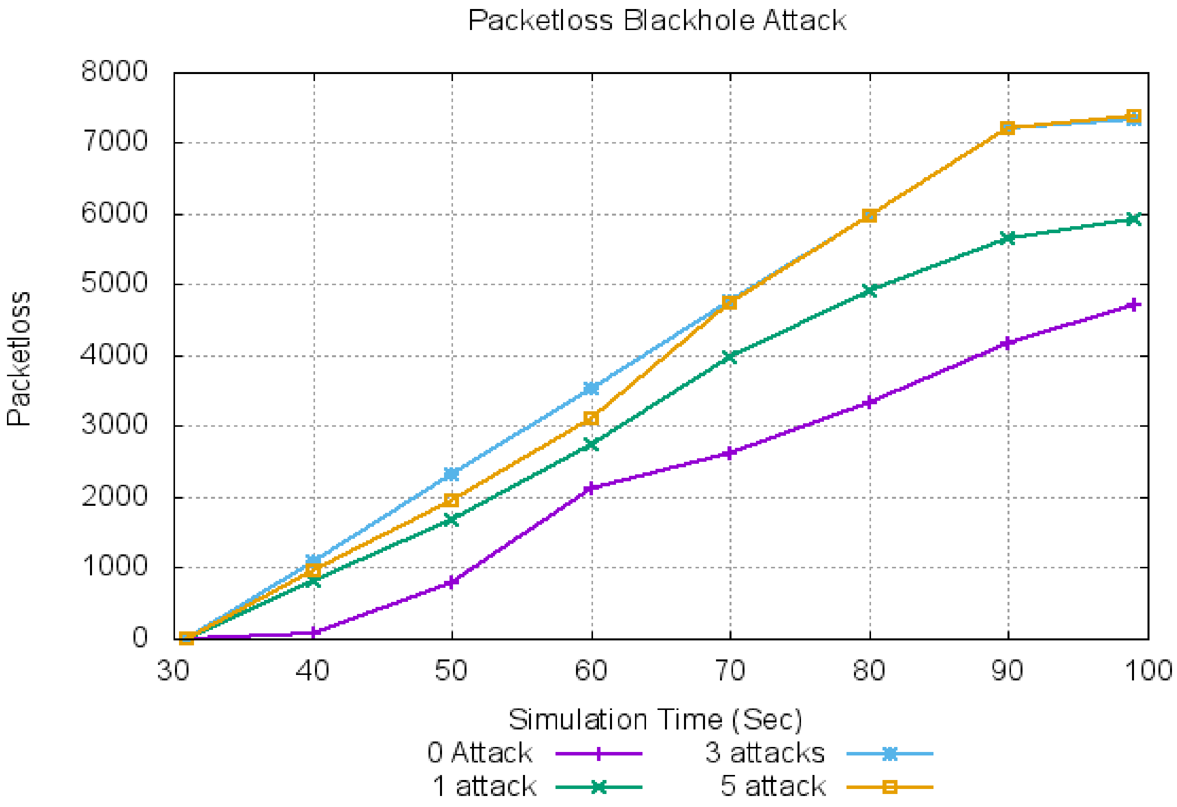


Figure 7:Simulation Time (Sec) Vs. Number of Packet loss**for0,1,3,5 black hole Attacks**

Table 3. Black Hole Attack: Simulation Time (Sec) Vs. Throughput

Simulation Time (Sec)	0 Black Hole Attack	1 Black Hole Attack	3 Black Hole Attacks	5 Black Hole Attacks
31	0	0	0	0
40	0.115012	0	0	0
50	0.137538	0	0	0
60	0.137832	0	0	0
70	0.143568	0	0	0
80	0.162806	0.0234582	0	0
90	0.175354	0.0837352	0	0
99	0.208786	0.136625	0.058649	0.0551349

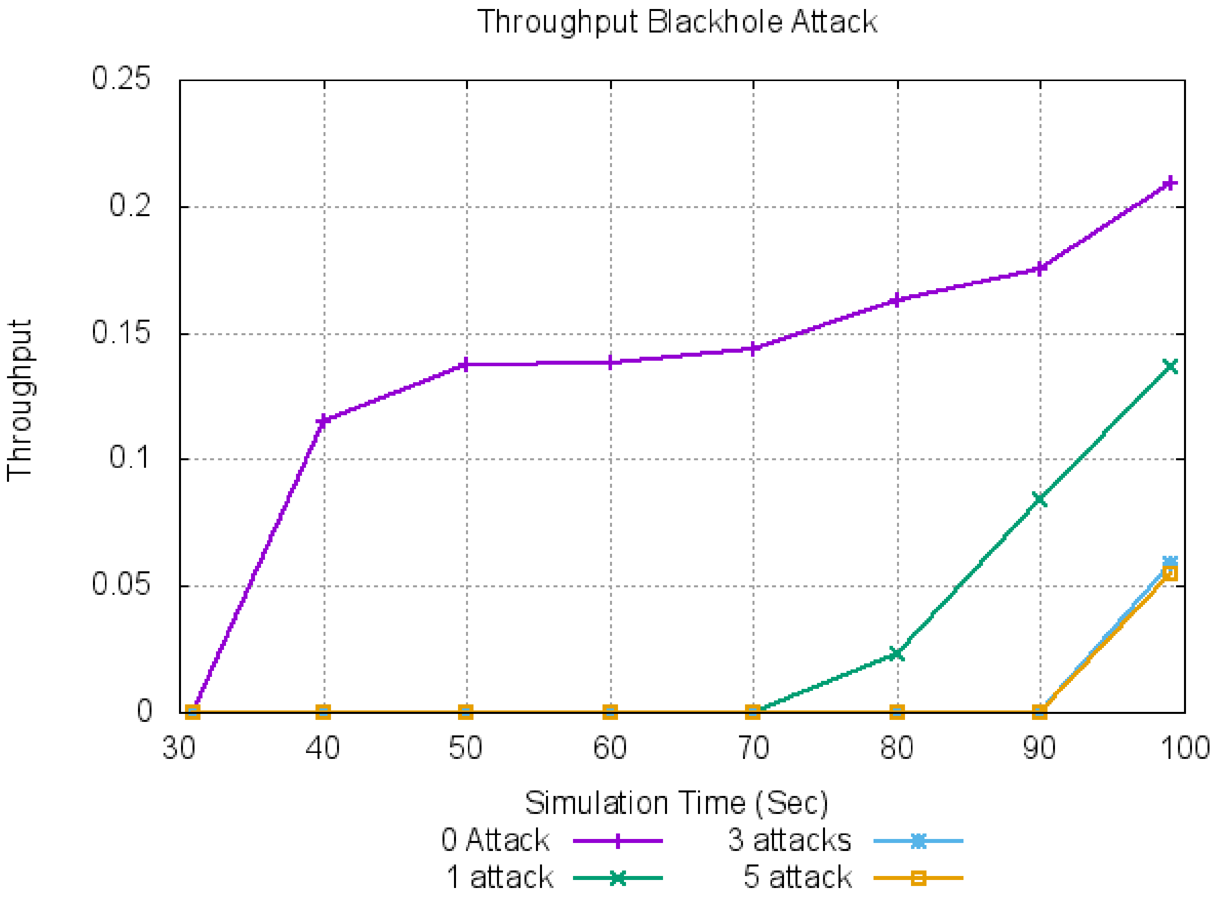


Figure 8. Simulation Time (Sec) Vs. Throughput**for0,1,3,5 black hole Attacks**

Table 4.Black Hole Attack: Simulation Time (Sec) Vs. Average End-to-End delay for each flow (ns)

Simulation Time (Sec)	0 Black Hole Attack	1 Black Hole Attack	3 Black Hole Attacks	5 Black Hole Attacks
31	0	0	0	0
40	9.72271e+08	0	0	0
50	1.17535e+09	0	0	0
60	1.10917e+09	0	0	0
70	1.05188e+09	0	0	0
80	1.03728e+09	4.6502e+08	0	0
90	9.74825e+08	5.2105e+08	0	0
99	6.93482e+08	3.14648e+08	4.8297e+06	4.84687e+06

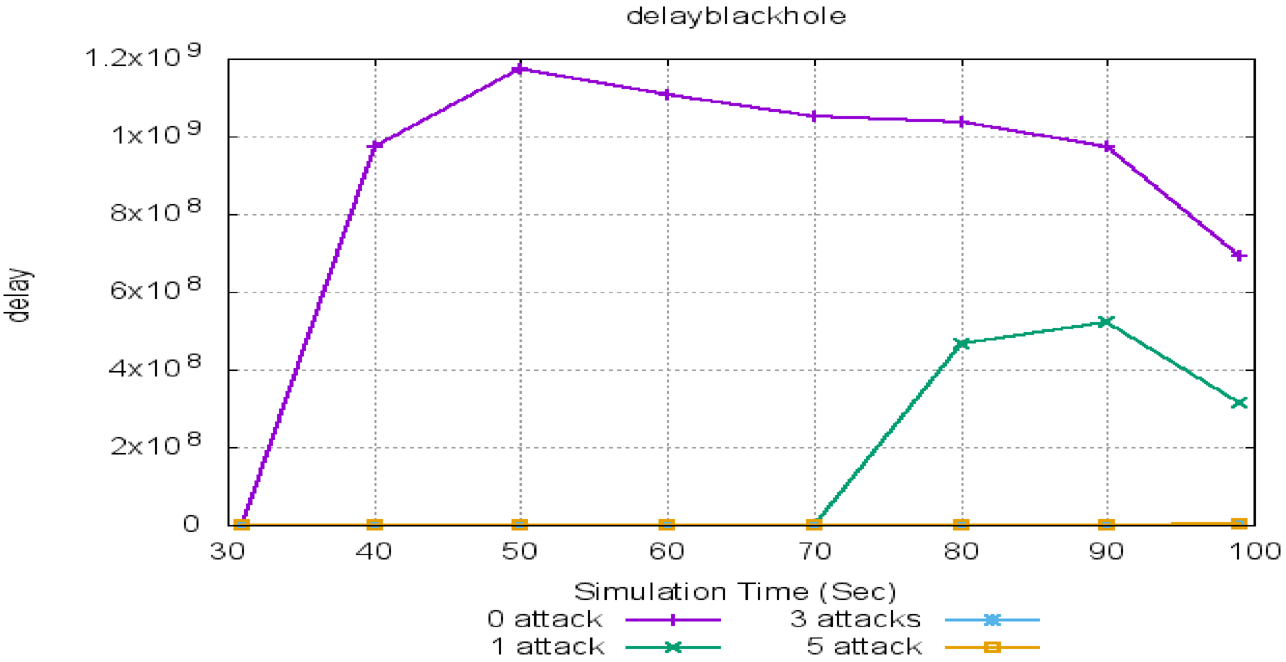


Figure9: Simulation Time (Sec) Vs. Average End-to-End delay for each flow (ns)

Table 5. Normal AODV and Black Hole AODV(0 Attack)

	Number of Packet loss		Throughput		Average End-to-End delay for each flow (ns)	
Simulation Time (Sec)	Normal AODV	0 Black Hole Attack	Normal AODV	0 Black Hole Attack	Normal AODV	0 Black Hole Attack
31	0	0	0	0	0	0
40	70	70	0.115012	0.115012	9.72271e+08	9.72271e+08

50	797	797	0.137538	0.137538	1.17535e+09	1.17535e+09
60	2122	2122	0.137832	0.137832	1.10917e+09	1.10917e+09
70	2610	2610	0.143568	0.143568	1.05188e+09	1.05188e+09
80	3334	3334	0.162806	0.162806	1.03728e+09	1.03728e+09
90	4168	4168	0.175354	0.175354	9.74825e+08	9.74825e+08
99	4707	4707	0.208786	0.208786	6.93482e+08	6.93482e+08

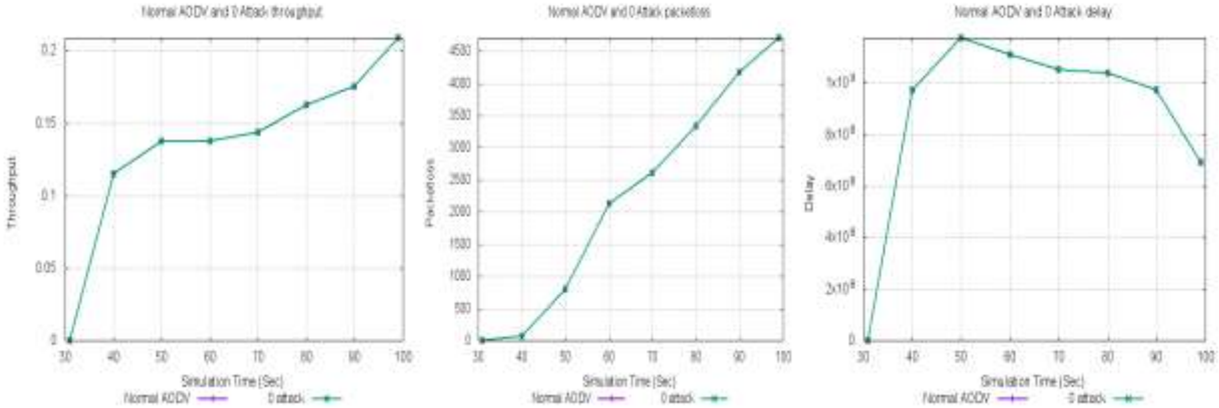


Figure 10: Normal AODV and Black Hole AODV with 0 Attack: Packet loss, Throughput and Delay

Table 6. Normal AODV and Black Hole AODV (1 Attack)

	Number of Packet loss		Throughput		Average End-to-End delay for each flow (ns)	
Simulation Time (Sec)	Normal AODV	1 Black Hole Attack	Normal AODV	1 Black Hole Attack	Normal AODV	1 Black Hole Attack
31	0	0	0	0	0	0
40	9	823	0.224671	0	5.24595e+08	0
50	581	1668	0.220323	0	7.61893e+08	0
60	1239	2737	0.223919	0	8.08441e+08	0
70	2140	3966	0.223823	0	8.60914e+08	0
80	2967	4915	0.217191	0.0234582	8.74647e+08	4.6502e+08
90	3449	5654	0.236404	0.0837352	7.84713e+08	5.2105e+08
99	3740	5925	0.268586	0.136625	6.20515e+08	3.14648e+08

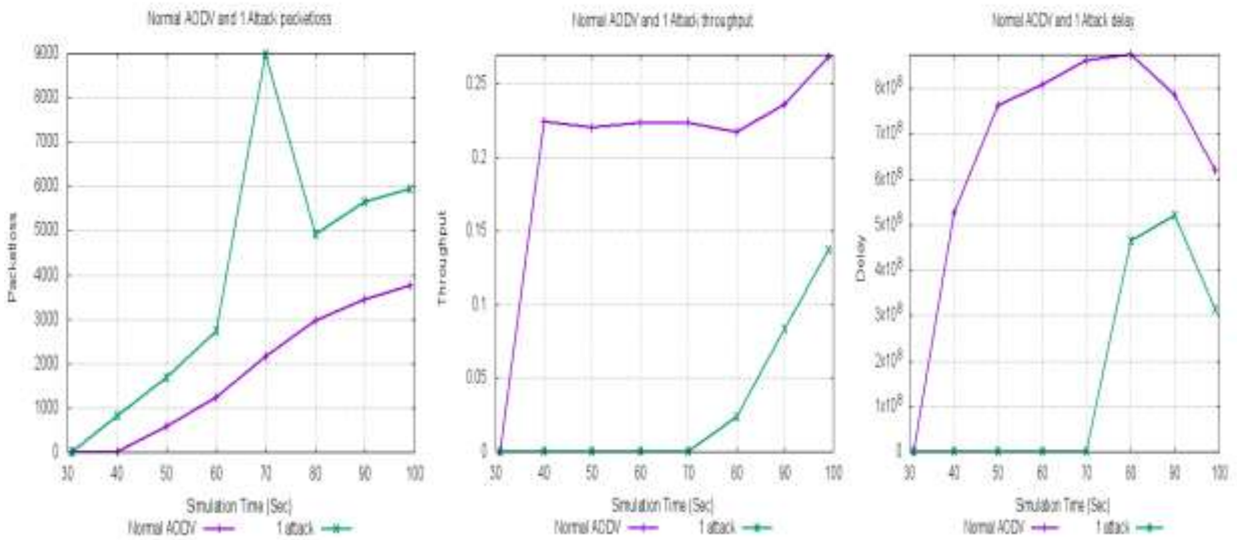


Figure 11:Normal AODV and Black Hole AODV with 1 Attack: Packet loss, Throughput and Delay

Table 7. Normal AODV and Black Hole AODV (3 Attacks)

	Number of Packet loss		Throughput		Average End-to-End delay for each flow (ns)	
Simulation Time (Sec)	Normal AODV	3 Black Hole Attack	Normal AODV	3 Black Hole Attack	Normal AODV	3 Black Hole Attack
31	0	0	0	0	0	0
40	279	1095	0.181895	0	5.61153e+08	0
50	628	2319	0.201128	0	8.85117e+08	0
60	1319	3540	0.212346	0	8.99983e+08	0
70	1977	4761	0.212346	0	9.43455e+08	0
80	2659	5981	0.219926	0	9.43482e+08	0
90	3437	7202	0.225085	0	8.96267e+08	0
99	3968	7333	0.249925	0.058649	6.9638e+08	4.8297e+06

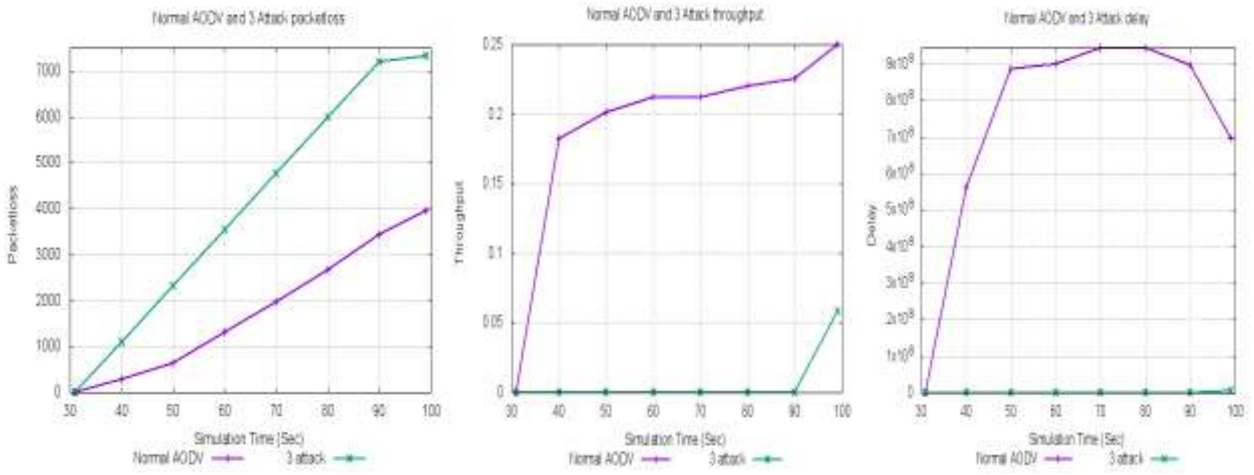


Figure 12: Normal AODV and Black Hole AODV with 3 Attacks: Packet loss, Throughput and Delay

Table 8. Normal AODV and Black Hole AODV (5 Attacks)

	Number of Packet loss		Throughput		Average End-to-End delay for each flow (ns)	
Simulation Time (Sec)	Normal AODV	Black Hole AODV (5 Attack)	Normal AODV	Black Hole AODV (5 Attack)	Normal AODV	Black Hole AODV (5 Attack)
31	0	0	0	0	0	0
40	415	959	0.155363	0	4.57098e+08	0
50	1004	1947	0.171979	0	7.27247e+08	0
60	1632	3101	0.189088	0	8.4923e+08	0
70	2297	4751	0.18903	0	8.97545e+08	0
80	2910	5981	0.194143	0	9.21468e+08	0
90	3632	7202	0.194279	0	9.28814e+08	0
99	4298	7391	0.225265	0.0551349	7.45856e+08	4.84687e+06

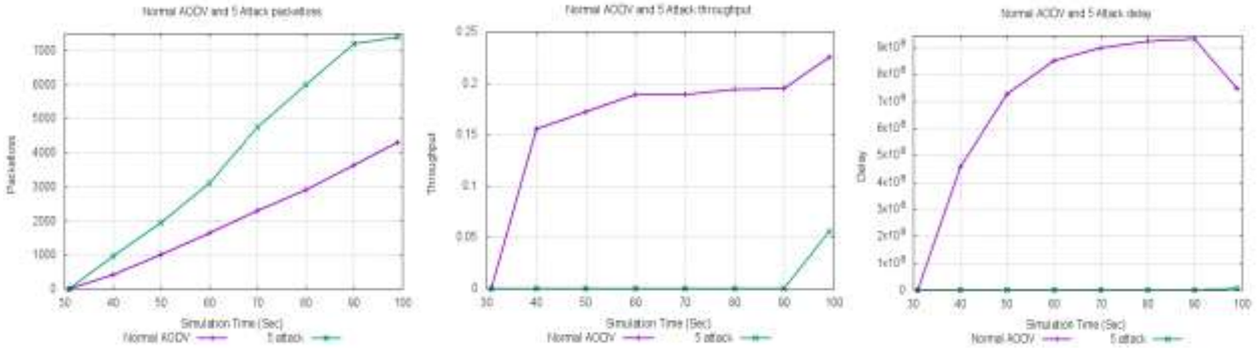


Figure 13: Normal AODV and Black Hole AODV with 5 Attacks: Packet loss, Throughput and Delay

4.1 Result Analysis:

As seen from the Figure 7-13 and Table 2-8; **Normal AODV and black hole; 0,1,3,5 Attacks black hole – Delay** for Normal AODV without black hole attack, delay is noticeable as it should be in the wireless network, while for 1- black hole attack, delay decreases due to attack; for 3 and 5 - black hole attack, delay is not noticeable as there is a more number of black hole attack.

As seen from the Figure 7-13 and Table 2-8; **Normal AODV and black hole; 0,1,3,5 Attacks black hole – Packet Loss** for Normal AODV without black hole attack, packet loss is less, while for 1- black hole attack, packet loss increases; for 3 and 5 - black hole attack, packet loss further increases.

As seen from the Figure7-13 and Table 2-8; **Normal AODV and black hole; 0,1,3,5 Attacks black hole – Throughput** for Normal AODV without black hole attack, throughput is high, while for 1- black hole attack, throughput decreases; for 3 and 5 - black hole attack, throughput further decreases.

Conclusion:

In this research paper, normal AODV algorithm, blackhole attack for 25 nodes with 0, 1, 3 and 5 blackhole attack scenario implemented using NS 3.26 latest version of network simulator 3.0on Ubuntu 16.04.2 LTS version platform. Comparison has been done regarding normal AODV and 0,1,3,5 black hole Attacks. Standard performance parameters like Delay, Packet loss and Throughput are taken for evaluation. Delay is not noticeable as there is a more number of black hole attack.packet loss increases as number of black hole increases. Throughput decreases as number of black hole attack increases.

REFERENCES

[1] Yahya Al-Harthi, Sem Borst and Phil Whiting, “Distributed Adaptive Algorithms for Optimal Opportunistic Medium Access,” Mobile Netw Appl (2011) 16:217–230, DOI 10.1007/s11036-010-0279-x.

[2] H. Huang, G. Hu,F. Yu and Z. Zhang, “Energy-aware interference-sensitive geographic routing in wireless sensor networks,” IET Communications, Vol. 5, Iss. 18, pp. 2692–2702, 2011.

[3] Samina Ehsan and Bechir Hamdaoui, “A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks,” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 14, NO. 2, pp. 265-278, SECOND QUARTER 2012.

[4] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, “Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey,” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, pp. 551-590, SECOND QUARTER 2013.

[5] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, “A Survey of Intrusion Detection Systems in Wireless Sensor Networks,” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, pp. 266-282, FIRST QUARTER 2014.

[6] 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.

[7] 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.

[8] 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.

[9] Hamid Al-Hamadi and Ing-Ray Chen, “Adaptive Network Defense 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.

[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] 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.*

[12] Neelam Janak kumar Patel and Dr. Khushboo Tripathi, “Sinkhole Attack Detection and Prevention in WSN & Improving the Performance of AODVProtocol,” 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.

[13] 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.

[14] Nguyen Cong Luong, Dinh Thai Hoang, Ping Wang, Dusit Niyato, Dong Kim, and Zhu Han, “Data Collection and Wireless Communication in Internet of Things (IoT) Using Economic Analysis and Pricing Models: A Survey,” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 4, pp. 2546-2590, FOURTH QUARTER 2016.

[15] Avinash More and Vijay Raisinghani, “A survey on energy efficient coverage protocols in wireless sensor networks,” Journal of King Saud University – Computer and

Information Sciences (2016) xxx, xxx–xxx, http://dx.doi.org/10.1016/j.jksuci.2016.08.001.

[16] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, "A Roadmap for Security Challenges in Internet of Things," Digital Communications and Networks, www.elsevier.com/locate/dcan, DOI: http://dx.doi.org/10.1016/j.dcan.2017.04.003.

[17] Mohammad Hammoudeh, Fayez Al-Fayez, Huw Lloyd, Robert Newman, Bamidele Adebisi,Ahcène Bounceur, and Abdelrahman Abuarqoub, "A Wireless Sensor Network Border MonitoringSystem: Deployment Issues and Routing Protocols," IEEE SENSORS JOURNAL, VOL. 17, NO. 8, pp.2572-2582, APRIL 15, 2017.