SECURING MANET FROM BLACKHOLE AND WORMHOLE ATTACKS

C.M.Vidhyapathi [#1],S.Sundar [#2], Harshita Pal [*3], Komal Punia [*4]
[#1] Assistant Professor, [#2]Assistant Professor (Sr), [*3&*4]B.Tech(ECE) Student,
[#&*] School of Electronics Engineering, VIT University, Vellore – 632014, Tamilnadu , India
[1]vidhyapathi.cm@vit.ac.in
[2]sundar.s@vit.ac.in
[3]hrshtapal@gmail.com
[4]komalpunia@vit.ac.in

Abstract: **Mobile Ad-Hoc networks are self-configuring and self-organizing multi-hop wireless networks. They do not have any fixed infrastructure or centralized management. Due to this, the ad hoc networks are vulnerable to attacks. The routing protocol for MANET considered in this paper is AODV(Ad hoc On-demand Distance Vector Routing Protocol). Blackhole and Wormhole nodes are malicious nodes which degrade the performance of the network. They actively participate in the network and conform to forward packets to the destination. The Watchdog Mechanism is used to correct the network from both blackhole and wormhole attacks. The networks originally, with the attacks and after being prevented from attacks are compared on the basis of *packets received, throughput, end-to-end delay and packet delivery ratio*. ns2 software is used for the simulation.**

Key Word—MANET, AODV, Blackhole and Wormhole attacks, Watchdog mechanism

I. INTRODUCTION

A Mobile Ad-Hoc Network(MANET) is a collection of autonomous mobile users communicating over bandwidth constrained wireless links[4]. Due to the mobile nodes, the topology of the network keeps changing unpredictably and rapidly over time. The network has no centralized management and therefore the nodes themselves discover the topology and deliver messages i.e. each node acts both as a host as well as router at the same time[4]. The mobile nodes communicate among the nodes outside the wireless transmission range by hop to hop and by forwarding packets to each other.

The primary goal of a MANET's routing protocol is to establish a correct and shortest route between the source and the destination[4].

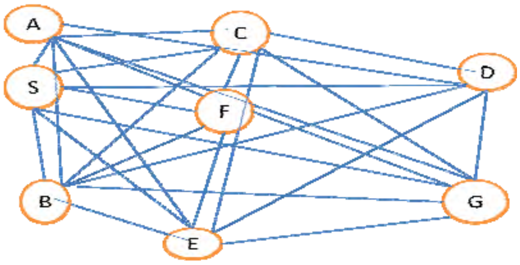

Fig.1. Mobile Ad-Hoc Network

If the routing is not effective, the entire network collapses[1]. Therefore, security of the network plays a very important role. The routing protocols are characterized as:

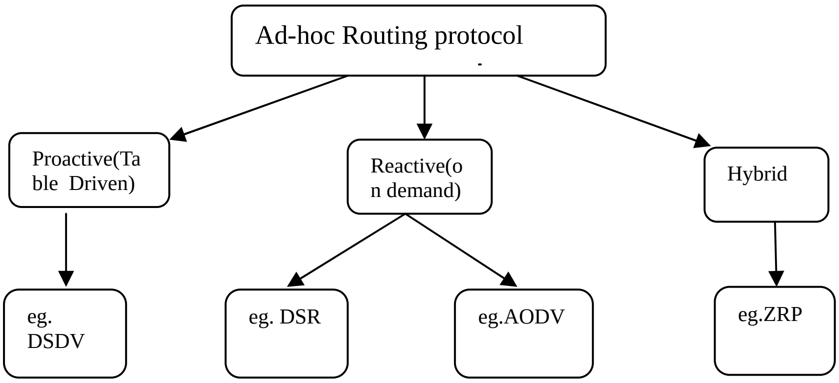

Fig.2. Characterization of the Ad hoc routing protocols

Proactive(Table Driven): This routing protocol maintains up-to-date routing information from each node to every other node in the network[6]. In this, each node maintains one or more tables which stores routing information. The tables are updated if there is any change in the network topology. Example: Destination Sequence Distance Vector(DSDV).

Reactive(On Demand): In this routing protocol, the routes are created only when desired by the source node. In order to establish a route to the destination when required, route discovery process is initiated within the network[6]. The process is completed once the proper route is found or all possible routes have been examined. Example: Dynamic Source Routing(DSR) and Ad Hoc On-Demand Distance Vector(AODV).

Hybrid Routing Protocol: The main idea here is to divide the nodes into different groups and providing them different functionalities inside and outside the group. Each group is known as cluster and each cluster has a cluster head(leading node) which communicates to other nodes outside the cluster. The nodes inside the cluster are proactive and all clusters altogether in a network are reactive. Example: Zone Routing Protocol(ZNR).

Due to lack of centralized monitoring nodes and dynamic infrastructure, the ad hoc networks are vulnerable to attacks. In this paper, two types of attacks on AODV routing protocol namely, blackhole and wormhole attacks are considered. These blackhole and wormhole attacks are removed with the help of Watchdog Mechanism, hence securing the MANET from these malicious nodes.

II. AODV ROUTING PROTOCOL

Ad-Hoc On Demand Distance Vector(AODV) falls in the category of reactive routing protocol. AODV create path to destination only when required. Routes are built only when certain nodes initiates route discovery process as on will to communicate or transmit data with each other. Only source node, destination node and intermediate node stores the routing information along the established route which deals with packet transmission[2]. This scenario has many advantages such as it decreases the memory overhead, minimizes the use of network resources and performs well in high mobility situations[8]. For the purpose of running algorithm AODV uses three types of control messages abbreviated as RREQ(route request), RREP(route reply) and RERR(route error) messages. The RREQ and RREP packet formats is shown below:

Source_address	Source_ sequence	Broadcast_Id	Destination _ address	Destination_ Sequence	Hop_Count

RREQ Field

Source_address	Destination_ address	Destination_ Sequence	Hop_Count	Lifetime

RREP Field

Fig.3. RREQ and RREP Fields

To establish the communication between source node and destination node, the source node issues the route discovery process. For this purpose RREQ broadcasts through source node to all it’s neighbors. The intermediate nodes checks the received RREQ[8]. If it is destined to the intermediate node, it replies with RREP.

If it is not the case, the RREQ will be forwarded to other neighbor nodes. The broadcast identifier and the previous node number from which the request came will be stored by each node before forwarding the packet. The intermediate nodes will use timers to delete the entry when no reply is received for the request. In case there is a reply, intermediate node will perform the task of storing the broadcast identifier and the previous nodes from which the reply came[8].

To detect whether the node has received the route request message previously broadcast identifier and source ID is used. This will prevent the redundant request receive in same node. If source node get more than one reply, it will determine later which message should be selected based on the hop counts[2]. In case of link failure, this can be due to the node mobility, the routing table will be invalidated by the node. This link failure will make all destination unreachable[2]. Then a route error (RERR) message which lists all of these lost destinations will be generated. Source node will get RERR sent upstream towards it by the node. After the source receives RERR, the route discovery process will be re-initiated if it still requires the route.

III. BLACKHOLE ATTACK

The Blackhole attack is a type of active insider attack. It is characterized by two properties: first, the attacker will consume all the intercepted packet without forwarding. Second, the malicious node will announce itself as an accurate route to a destination node, where in reality it is not, thus exploiting the ad-hoc routing protocol[7]. In ad-hoc network that uses AODV protocol for routing, a black-hole node assumes to have a fresh enough routes to all destination requested by all the nodes and absorbs the network traffic. When a source node broadcasts RREQ messages to set a route to destination, the blackhole node instantly replies with an RREP message and this received message is considered to be as if it is coming from the destination or from a node which has a fresh route to the destination[8]. The source node assumes that the destination is next to the node from where the RREP came first(i.e. the blackhole node) and does not consider the RREP packets coming from other nodes. The source then starts to send out its data packets to the blackhole node, considering that these packets will reach the destination[8].

For example, consider node B to be malicious blackhole node. Using AODV routing protocol, whenever node B receives any RREQ packets it claims that it has the route to the destination node and replies to the source node with RREP immediately. The destination node may also reply to source node with RREP. If the reception of RREP from normal destination node is before the reception of RREP from blackhole node, everything works well.

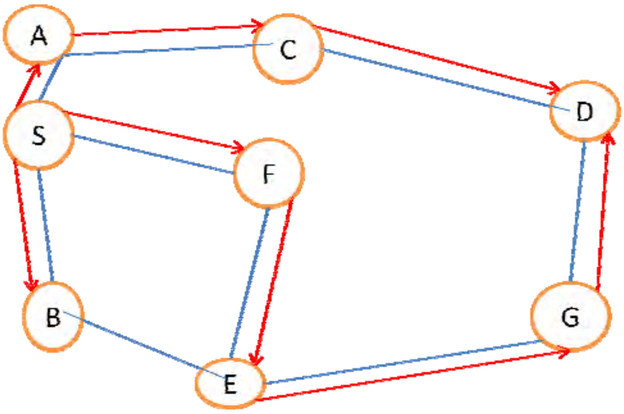

Fig.4. RREQ messages broadcasted

But in case where B is physically close to source, then reply from B will reach the source node first. The source node will assume that the route discovery process is completed, hence it will ignore all other reply messages, and will start transmitting data packets. The malicious route has been established. As the consequences, B will consume all the packets passing through it. This node B has created a blackhole in the network and this is called blackhole attack.

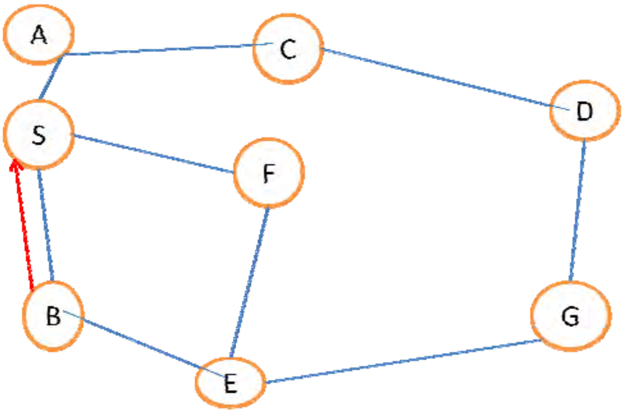

Fig.5. RREP message propagation

IV. WORMHOLE ATTACK

In wormhole attack, the usual flow of routing packets is short circuited to disrupt routing. This type of attack can be materialized with one node also. But usually, two or more malicious nodes connect via a link known as “wormhole link”[9]. The private high speed network is used by these malicious nodes to capture packets at one end and replay them at the other end[9]. Fake packets are sent to the destination via wormhole nodes. The acknowledgments through the wormhole link is very high as it intends to receive more packets. This type of attack is relatively easy to deploy than other attacks but may have serious damage to the network[9]. It can be very effective and damaging even in the case when routing information is confidential, encrypted or authenticated. In this type of attack, the attacker will tunnel route request packet RREQ directly to the destination node without increasing the hop count value. Thus discovery of other route is prevented. Therefore, AODV will not find any routes longer than one or two hops. Attacker tunnels the arrived packets with better accuracy than a normal multi-hop route for tunneled distance longer than the typical transmission range of single hop. The retransmission of eavesdropped messages in a channel that is exclusively available to attackers can be performed by malicious node[9]. The message dropping attack can be combined with this attack to prevent destination node from receiving packets.

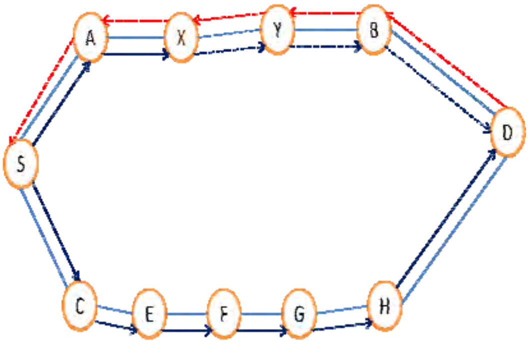

Fig.6. Wormhole Attack

Wormhole attack consists of two distant malicious nodes depicted as X and Y in Figure 6. X and Y are connected via a wormhole link and have a goal to attack the source node. In route finding process, S broadcasts RREQ, A and C receives RREQ and forward it to their neighbors. The malicious node X is the neighbor of A and now node X will receive RREQ. X updates and tunnels the RREQ through the high speed wormhole link to its associate Y. B is neighbor of Y, so Y will forward it to B.

At last, B forwards it to destination D. Thus,RREQ is transmitted from node S to destination D through S-A-X-Y-B-D. As X and Y are connected via high speed link so RREQ from S-A-X-Y-B-D reaches first to D. So, the later arrived RREQ packets will be ignored by destination D. The route D-B-A-S is considered to uni-cast a RREP packet to the source node S. The route S-A-B-D chosen by the source node S consists of high speed link connecting malicious nodes X and Y that are very well placed compared to other nodes in the network. The materialization of wormhole attack is not a cumbersome task, but it can have serious damage to the network.

V. WATCHDOG MECHANISM

To analyze the effect of malicious nodes i.e. blackhole and wormhole, the wireless ad hoc network is simulated with and without the presence of these malicious nodes[10]. In order to secure the network from the blackhole and wormhole attacks, the new protocol is designed. In this, two extra tables are added to each node. For the detection blackhole attacks, the two tables are pending packet table and node rating table. The fields of pending packet table is shown below:

Packet ID	Next Hop	Expiry Time	Packet Destination

Fig.7. Pending Packet Table

- First field: Packet ID- ID of the packet sent
- Second field: Next Hop- Address of the next hop node
- Third field: Expiry Time- Packet lifetime
- Fourth field: Packet Destination- Address of the destination node

The fields of Node Rating Table are as follows:

Node Address	Packet Drops	Packet Forwards	Misbehave

Fig.8. Node Rating Table (for detection of blackhole)

- First field: Node Address- Next hop node's address
- Second field: Packet Drops- The dropped packet counter
- Third field: Packet Forwards- The forwarded packet counter
- Fourth field: Misbehave- It can take two values, either 0 or 1, 0 is assigned for well behaving node, and 1 is assigned for misbehaving node.

The Node Rating table is updated according to Pending Packet table. In Watchdog Mechanism, each node keeps track of every packet it sends through pending packet table. The rating of nodes which are within its communication range is maintained by each node with the help of node rating table.

The misbehave value for the blackhole is calculated by the ratio of dropped packets and successfully forwarded packets. If the ratio exceeds the give threshold value then the node's misbehave value will be set to 1. Indicating that the node is a blackhole node. If the misbehave value is 0 then it means it is a legitimate node. The packet drop counter of pending packet table increases if it has an expired packet in table for the next hop correlated with the pending packet table entry.

In case of wormhole node detection, the pending packet table remains the same while the node rating table is changed slightly. This is shown below:

Node Address	Packet Forwards	Acknowledgments	Misbehave

Fig.9. Node Rating Table (for detection of wormhole)

The misbehave value for this is calculated by the ratio of acknowledgments and successfully forwarded packets. If the ratio exceeds the give threshold value then the node's misbehave value will be 1, indicating that the node is a wormhole node. If the misbehave value is 0 then it is a legitimate node.

VI. ALGORITHM

6.1. AODV Routing Protocol

a. Nodes are configured and created:

1. Channel type: Wireless Channel
2. Radio-propagation model: Two Ray Ground Model
3. Antenna type: Omni Antenna
4. Link Layer type: LL
5. Interface Queue type: DropTail/ PriQueue
6. Maximum packet in ifq: 200
7. Network Interface type: WirelessPhy
8. MAC type: 802.11

9. Number of mobile nodes: 50
10. Routing Protocol: AODV
11. Network Dimensions: x- 500,
y- 500

b. Setting the nodes' size and initial positions.
c. Giving mobility to the nodes.
d. Setting the animation rate as 15ms.
e. Setting tcp connection between nodes with constant bit rate traffic type.
f. Packet Size: 500 bytes
Simulation time: 10s
Time interval between consecutive packets: 0.05us
Data extracted at the interval of: 2s
g. Performance evaluation on the basis of:
1. Packets Received
2. Throughput
3. End-to-end delay
4. Packet Delivery Ratio

6.2. Blackhole and Wormhole attacked network

a. Nodes are configured and created.
b. Setting the nodes' size and initial positions.
c. Giving mobility to the nodes.
d. Setting the animation rate as 15ms.
e. Setting tcp connection between nodes with constant bit rate traffic type.
f. Packet Size: 500 bytes
Simulation time: 10s
Time interval between consecutive packets: 0.05us
Data extracted at the interval of: 2s
g. For the Blackhole attack, the threshold value of two nodes are increased so that they behave as blackhole nodes.
h. For the Wormhole attack, the acknowledgments of two nodes are increased and a high speed link is set between them such that they behave as wormhole nodes.

6.3. Watchdog Mechanism for Blackhole:

```
a.      Data packet sent or forwarded.
b.      Data packet kept in the pending packet table until it is forwarded or gets expired.
c.      If(data packet is forwarded)
{
Forwarded packet in the node rating table is incremented.
Data packet is removed from the pending packet table.
}
d.      If (data packet expires)
{
Dropped packet in the node rating table is incremented.
Data packet is removed from the pending packet table.
If(packet dropped > threshold)
{
If(misbehave > threshold)
{
Misbehaving node.
Other nodes are informed of the malicious node.
RREP coming from the node is discarded.
}
}
}
```

6.4. Watchdog Mechanism for Wormhole:

```
a.      Data packet sent or forwarded.
b.      Data packet kept in the pending packet table until it is forwarded or gets expired.
c.      If(data packet is forwarded)
```

```
{
Forwarded packet in the node rating table is incremented.
Data packet is removed from the pending packet table.
If(acknowledgment > threshold)
{
If(misbehave > threshold)
{
Misbehaving node.
The other nodes are informed about the malicious node.
RREP coming from the node is discarded.
}
}
}
```

VII. SIMULATED RESULT

The red lines represents the original AODV, green lines represents the blackhole and wormhole attacked AODV and the blue lines represents the AODV secured by the Watchdog Mechanism. The simulations are done using ns2.

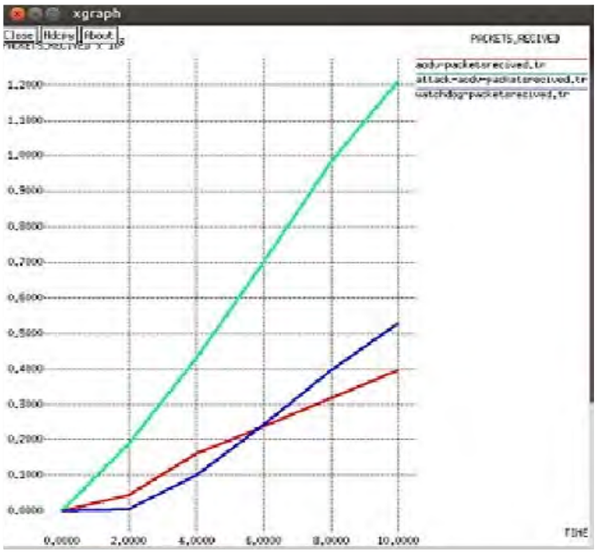

Fig.10. Packets received Vs Time

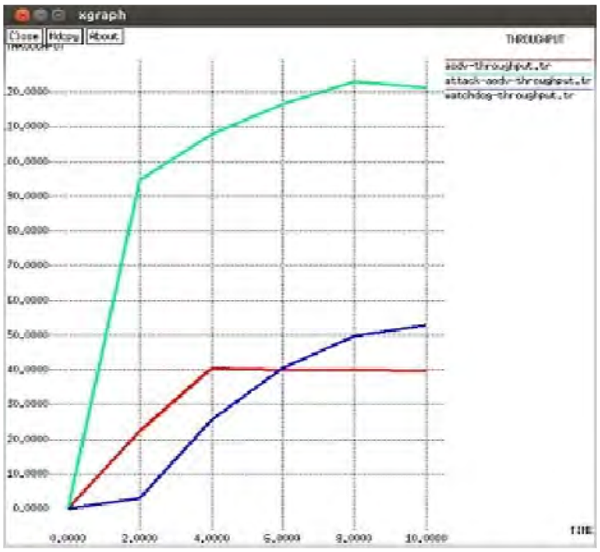

Fig.11. Throughput = Total no. of packets received/Total traversing time

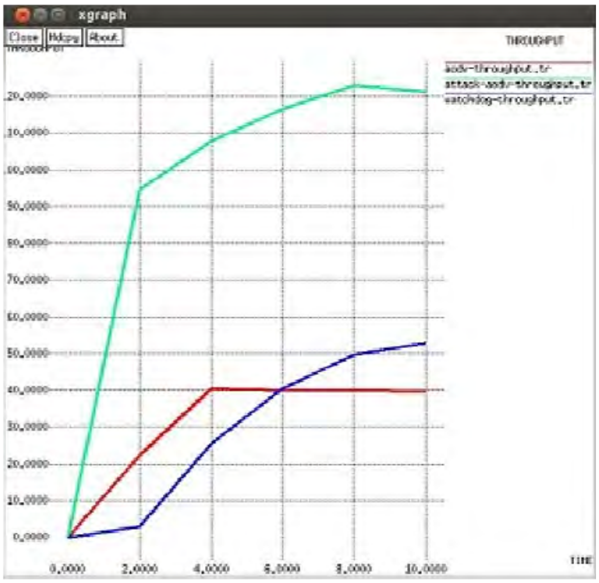

Fig.12. End-to-end delay = Receiving time – Sending time

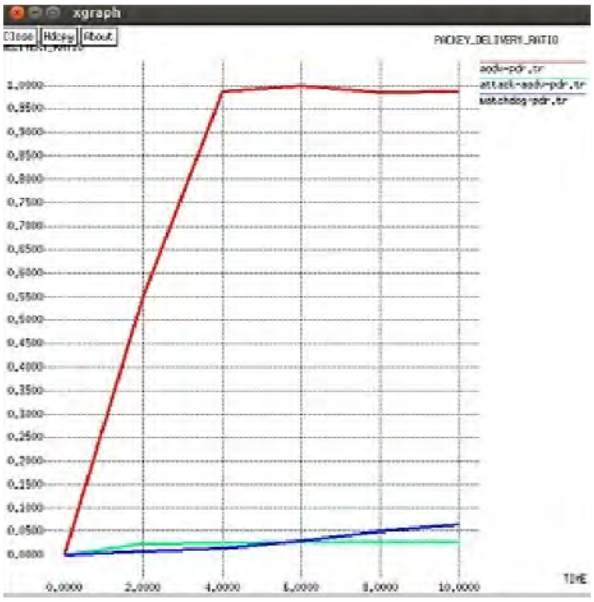

Fig.13. Packet Delivery Ratio = Total no. of packets received/Total no. of packets send

VIII. CONCLUSION

Ad hoc routing protocols are vulnerable to a variety of attacks which influences a victim's selection of routes. In this paper, two types of attacks were implemented in the network, blackhole attack and wormhole attack. The effect of these attacks on the network were analyzed on the basis of packets received, delay, throughout and packet delivery ratio. Then Watchdog Mechanism was used in order to secure the network from these attacks. Finally, the comparison of the original AODV, attacked AODV and secured AODV was done considering again the same four parameters *packets received*, *end-to-end delay*, *throughout*, *and packet delivery ratio*. It is clear from the results that Watchdog mechanism is very effective in securing the network from blackhole and wormhole attacks.

REFERENCES

[1] Amol A. Bhosle, Snehal Mehatre and Tushar P. Thosar, *“Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”*, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol. 2, No. 1, February 2012.

[2] Elizabeth M. Royer and Charles E. Perkins, *“Ad Hoc On Demand Distance Vector Routing”*, Dept of Electrical and Computer Engineering, University of California, Santa Barbara, 2008.

[3] David A. Maltz and David B. Johnson, *“Dynamic Source Routing in Ad Hoc Wireless Networks”*, Computer Science Dept., Carnegie Mellon University, 2004.

[4] Imrich Chlamtac, Jennifer J. – N. Liu, Marco Conti, *“Mobile Ad Hoc Networking: Imperatives and Challenges”*, School of

Engineering, University of Texas at Dallas, Dallas, TX, USA, 2003.

[5] Zaiba Ishrat, *“Security Issues, Challenges and Solutions in MANET”*, International Journal of Computer Science and Technology, Vol. 2, Issue 4, Oct-Dec. 2011.

[6] Hongmei Deng, Dharma P. Agarwal and Wei Li, *“Routing Security in Wireless Ad Hoc Networks”*, University of Cicinnati, IEEE Communication Magazine, October 2002.

[7] Saurabh Gupta, S Dharamaraja, and Subrat Kar, *“BAAP: Blackhole Attack Avoidance Protocol for Wireless Network”*, International Conference on Computer & Communication Conference (ICCCT)- 2011.

[8] Anu Bala, Jagpreet Singh, Munish Bansal, *“Performance Analysis of MANET Under Black-Hole Attack”*, First International Conference on Networks & Communications, 2009.

[9] Rutvij H. Jhaveri,Jatin D. Parmar, Ashish D. Patel, Bhasin I. Shah, *“MANET Routing Protocols and Wormhole attack Against AODV “*, International Journal of Computer Science and Network Security, Vol. 10, No. 4, April 2010.

[10] Youngho Cho and Gang Qu and Yuanming Wu, *“Insider Threats Against trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks”*, IEEE CS on Security and Privacy Workshop, 2012.