ISSN:0975-9646

Wormhole Detection and Prevention Scheme using Beacon Node Mechanism with Neighbor Node Discovery

Akansha Agrawal
Computer Science & Engineering
TRUBA Institute of Engineering & Information Technology
Bhopal, India

Prof. Amit Saxena
Computer Science & Engineering
TRUBA Institute of Engineering & Information Technology
Bhopal, India

Abstract—- **The wormhole attack is considered a serious threat to the security in multi-hop ad hoc networks. In wormhole attack, the attacker makes the tunnel from one end to another network, the nodes are in a different place at both ends of the tunnel believe are true neighbours and gets the conversation through the wormhole link . Unlike many other ad hoc routing attacks, worm hole attack cannot be prevented by cryptographic solutions because intruders or create new or modify existing packages, but before existing. In this paper a simple technique to effectively detect attacks wormholes without any special hardware and / or location or timing of the stringent requirements proposed. The proposed technique allows the use of the variance in routing information between neighbours to detect wormholes. Basic thesis is to find the alternative path from the source to the second jump and calculate the number of hops to detect wormhole.**

***Index Terms*—: MANET network, wormhole, threshold, AODV**

I. Introduction

An ad hoc network does not have a network infrastructure. This is a network which is spontaneously formed in order to meet the immediate need for communication between mobile nodes. Mobile ad-hoc network is operating in ad hoc manner. A mobile ad hoc network is a set of nodes that are able to change their position randomly, but can communicate. Coordinate with other nodes there no centralized device available. These nodes are able to send and receive data on their own. They can also perform routing. And the Ad-hoc network is very popular due to unstructured network. Due to this assets, there are so many practical application used in this time.

It can be used by the military. The border is the most sensitive area that communication must take place 24 hours. But at some point it is necessary to establish a network of instant communication. Time for Ad-hoc network plays an effective role A mobile ad hoc network (MANET) is a collection of wireless mobile nodes forming a dynamic autonomous network through a mobile infrastructure fully. This network is free of any fixed infrastructure or centralized administration. A node communicates directly with other nodes within range wireless communication without the intervention of centralized access points or base stations.

Mobile ad hoc network is a network configuration which is self-formed automatically by a plurality of mobile nodes without the use of a fixed infrastructure or centralized administration. Each node is prepared with a wireless transceiver that enables communication with other nodes in its range. For a node to send a packet to a node that is within its radio coverage area the support of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as a router and host at the same time. The topology of the network changes usually due to the mobility of mobile nodes in the network

II. Security Constrains In Manet

MANET vulnerable to various types of attacks. Some attacks affect to general network, some affect to wireless network, and some are particular to MANETS. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks [3]. These security attacks in MANET and all other networks can be generally classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

III. WORM HOLE ATTACK

Wormhole Attack is a serious threat in MANET. In wormhole attack two malicious nodes which are geographically highly separated to each other present an illusion to rest of network that they are neighbor node and try to attack maximum traffic of network. Once the any node fall into their illusion send their data packet via them they can either scan, change or drops the entire confidential message inside the packet in the time of journey of packet over the wormhole tunnel. Generally wormhole puts their malicious nodes at powerful position within the network as compared to other nodes so its attack maximum traffic of network and prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed [7].

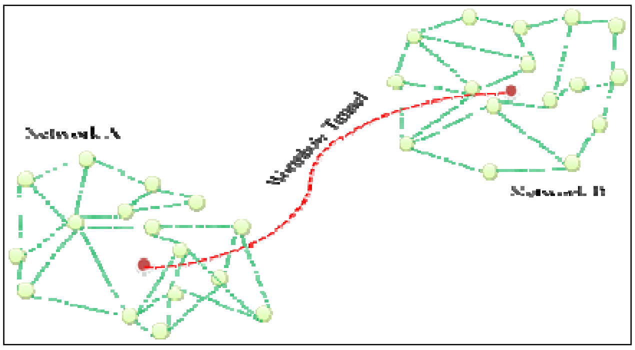

Figure 1: Wormhole in MANET Network

IV. WORMHOLE ATTACKS AND ITS TYPES

There are three types of wormhole attacks. These are classified on the basis of its Nodes. There are open wormhole attack, half open wormhole attack and closed wormhole.

- **Open Wormhole Attack**: In this type of attack both nodes in the network are available to complete the communication in the network. The two nodes can modify the data and show them self in the way of route discovery.

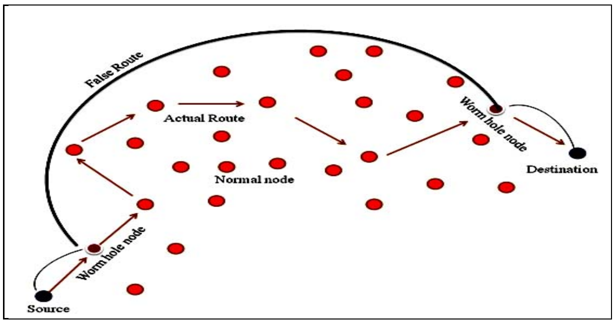

Figure 2: Open Wormhole Attack

- **Half Open Wormhole Attack:** In this type of attack only one node of wormhole malicious node in the network is open to spoil data integrity.

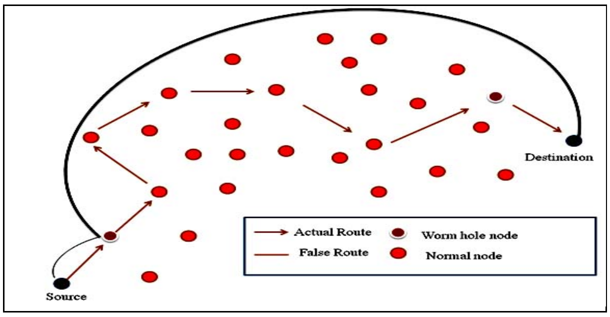

Figure 3: Half Open Wormhole Attack

- **Closed Wormhole Attack:** When the tunnel has formed then both node hide them self from the network but act for modifying the data. They show the shortest path to send the data.

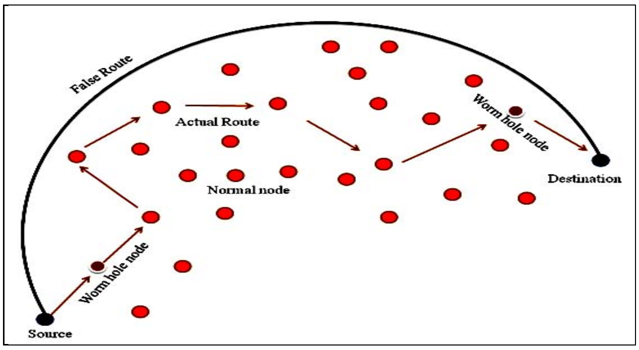

Figure 4: Closed Wormhole Attack

V. RELATED WORK

In recent year number of technique has been proposed for the wormhole detection. The proposed work [9] has developed the novel protocol in order to prevent the wormhole attack in the wireless environment. The author has used the symmetric and asymmetric key cryptography with Global positioning system. The protocol has tested on the both GPS node and non –GPS node. The author has tested the protocol with the ratios of GPS nodes to non-GPS nodes 30:20, 25:25, and 20:30, 15:35, 10:40 and 5:45 under a total network area of 100 by 100 meters. This gives the higher results.

The author [10] has proposed the novel approach say RTT-TC that is round trip time measurements and topological comparisons. They have used the AODV routing protocol. First of all the author applies rely on RTT measurements in order to get the suspected wormhole attack and then use the topological comparison approach to real neighbours from the suspected list. Simulation and the results shows that the proposed approach has given a higher detection rate and accuracy of alarms.

The author [11] has proposed a protocol which doesn't uses any special hardware like directional antenna or synchronized clock. This protocol doesn't depend on the physical medium of the wireless network. In this approach the wormhole detection will take place after the discovery of route. Here the hope count techniques have also used between neighbours. The author has also applied the hound packet. The simulation results show that the WHOP is quite excellent in detecting wormhole of large tunnel lengths.

The digital signature is a popular approach to secure the data. In this paper [12] the author has used the Digital signature to defend the wormhole attack. A digital signature has used to verify the sender and the receiver node. Here each legitimate node in the network contains the digital signature of every legitimate node of the same network. Now if the sender wants to send the data then first of all they have to create the secure path. The digital signature will help to create this secure path in the network with the verification. This identification approach will help to find the malicious node from the network. Number of packets, throughput and over head level are compared in this approach which is batter then the previous methods.

The wormhole is a major problem in mobile ad-hoc network. For the best result there are many protocols has developed. The two famous protocols are AODV and DSR. This paper [13] gives the comparison result between these protocols. The parameter considered by the author are: packet delivery fraction, the average end-to-end delay, average jitter, throughput, number of frames tunnelled, number of frames intercepted, number of frames dropped, number of frames replayed etc. the results shows that AODV is perfect protocol for the small network. Due to the routing overhead of AODV the performance will decrease in large network. But As the length of colluding link increases, the performance for DSR degrades compared to AODV.

It is seen that the majority of previous approaches to detect wormhole shows performance and fell on the higher complexity. As mobile nodes operate with limited battery power, so that the development of a technique that can successfully defend against the attacks of wormholes is very necessary, while maintaining low complexity. The objective of this work is to develop a new approach that can successfully defend themselves against attacks wormholes and consume less energy for longer survival of MANET and the battery MANET network.

VI. PROPOSED METHODOLOGY

Proposed methodology of wormhole detection and prevention is based on beacon node Based scheme [4] and neighbor node based solution of wormhole problem. The main theme of the proposed technique is to discover wormhole in the route suggest by AODV protocol by using an divide and conquer technique in which wormhole detection is performed between all the possible combination of node to its next to next node and decision will be taken on the basis of each and every possible combination if wormhole is detected in any of possible combination then whole suggested path is consider to be as wormhole effect path elsewhere if all the combination is wormhole free then path is consider to be as worm hole free path. In proposed methodology every node responsible to find out, is there any worm hole between that node to its next to next node? For detection every node find alternate route for its next to next node as suggested by AODV expect via AODV suggest , if number of hop count in any of alternate route is greater than threshold than that node reply wormhole detection signal between itself and its next to next node . Algorithm for wormhole detection is described below in algorithm 1.

Some primary assumptions are considered in the proposed approach:

- All communications are within the fixed radio range and all the communication links are bi-directional.
- All nodes in the network have same transmitting and receiving signal strength.
- Mobility does not influence the algorithm but for the accurate result of simulation it is assumed that nodes are stable or have zero mobility.
- Threshold value for detecting the wormhole totally depends on the network density.

The fundamental scheme of the method is to determine another routes to a detecting node D that is two-hop neighbor's nodes from beacon node. These alternative routes will be extensively dissimilar in length, means the length of the alternative path is greater than the path that have wormhole, and otherwise the wormhole will not attract large amounts of traffic. Consider a source-destination pair communicating node (S, D), with an route RS,D . If node S wants to detect the existence of a wormhole, S discovered a new route to T and if the length new route varies widely in comparison to the length of PS, T (that is, greater than a threshold), it is concluded that there wormhole.

Consider a situation in which the source route found by any routing protocol is S->1->2->3->4->5->6->7->8->9->D (as shown in figure 4.3) which is the legal path.

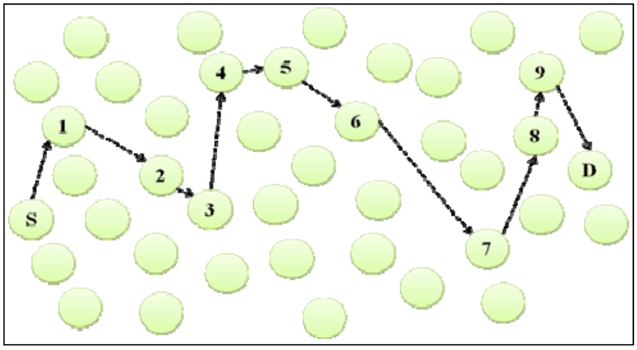

Figure 5:-Legal source route found by routing protocol

With the introduction of closed wormhole attack in the legal source route, the new malicious route will be S->1->2->8->9->D.

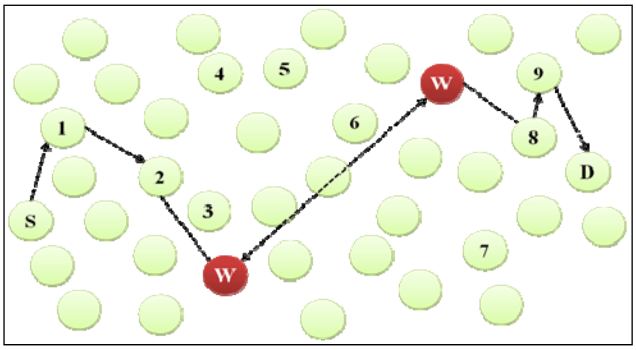

Figure 6: Malicious route containing Wormhole

As the proposed approach for detection of wormhole solely depends on the density of nodes in the network, therefore the value of threshold must be predefined. The threshold value is calculated by checking the average number of hops between the nodes in the network. In the situation defined in figure 4.4, the value of threshold is calculated as 5.

Now, in order to detect the wormhole, the proposed approach tries to find the number of hops in the shortest path between two nodes seconds replacement source S. If the number of hops in the second shortest is more than the predefined threshold, then indicates that wormhole is present between the two nodes.

For example the malicious path containing the closed wormhole is S->1->2->8->9->D.

Now proposed algorithm will check the number of hops found in the second shortest path between the nodes S and 2. In the situation given in figure 4.4, second shortest path between S and 2 will S->a->b->c->2. Now the number of hops between S and 2 is found to be 3 which is less than predefined threshold (i.e. 5), it is declared that no wormhole is present between the nodes S and 2. The same algorithm is followed by next two nodes (i.e. 1 and 8). As the number of hops in the second shortest path from node 1 to 8 is greater than the predefined threshold, therefore it the presence of wormhole is declared between the nodes 1 and 8.

VII. PROPOSED ALGORITHM

In proposed algorithm all decision will be taken on the basis of value of maximum hop distance i.e. maximum number of hop distance in alternate route between every pair of beacon node and detecting node is discover by AODV. If it’s greater than maximum hop distance, then it’s declared there is wormhole between beacon node and detecting node, elsewhere not.

Algorithm for Wormhole Detection and Prevention Assumption

Node[i] = List of over the network

Radio $node_j^{Ni}$= Radio node of Node[i]

N_i^b = Beacon node, which responsible to detected wormhole

N_i^d = detecting node

$hope_{distance}[j]$ = Array that store hop distance

$Network_{mhd}^{node[j]}$ = Maximum hop distance between beacon node and detection node

```
Algorithms
{
Step 1:- Any random source node (S) broadcast route request packet to all there radio node path towards their desired destination (D) as per AODV
Step 2:- AODV reply Route reply packet (RRP) with route R
R= n0, n1, n0… nm
Where
n0= source node
nm= destination node
Step 3:-
For (i=0;  i<) nm-2; i++)
{
    $N_i^b = //_{select\ ni\ a\ sbeacon\ node}$
    $N_i^d$ = ni + 2// select ni + as detecting node
    For ( j = 1; j <= $^{Radio\ node_j^N}$ ; j++ ;)
    {
        $N_i^b$ Broaddcast RRP for $N_i^d$
        Radio $node_j^{Ni}$ reply hop distance between $N_i^b$ & $N_i^d$
        $hope_{distance}[j]$ = hop distance
    }
    $if\,(\,maxhope_{distance}[j] \;>\; Network_{mhd}^{node[i]})$
    Than
    Reply wormhole is present in route
    Exit ();
    Else
    Go to Step 3
}
Reply route R is selected for transmission
}
```

In proposed methodology main focus on how to calculate maximum hop distance of the network for a fixed number of node. Proposed methodology use an evolutionary model that use beacon node concept along with neighbor node concept. In beacon node concept every node have a GPS system to coordinate their position over the network but use very large amount of battery power, this is bottle nick of this system.

To overcome this demerit proposed methodology combine the feature of neighbor node information scheme with beacon node scheme in order to overcome the demerit of both being alone. In proposed methodology for calculating maximum hop distance each and every node behave like beacon node and find the path having the largest number of node over the entire possible path between it and it’s detecting node and consider average value highest hop distance of the entire node as maximum hop distance over the network as describe in algorithm 2

Algorithm for Maximum hop distance between beacon node and detecting node ($Network_{mhd}^{node[i]}$)

```
Algorithms
{
For (  i = 1 ; i<= n ; i++)
{
    $N_i^b = //_{select\ ni\ a\ sbeacon\ node}$
    Max (HC)i = 0
    For ( j = 1; j <= $^{Radio\ node_j^N}$ ; j++ ;)
    {
        For ( k = 1; k <= $^{Radio\ node_k^{Ni}}$ ; j++ ;)
        {
$N_k^d$ = nk//Select nk as detecting node
$N_b^i$= broad cast RRP for $N_k^d$
hop distance < -- Aodv Reply for $N_k^d$
}
}
}
$Network_{mhd}^{node[i]} \quad = \quad \frac{\sum_{i=1}^{n} Network_{nd}^{node[i]}}{n}$
}
```

VIII. SIMULATION AND RESULT ANALYSIS

The performance of proposed algorithm has analyzed through a number of simulation tests in network simulation. The simulation results showed that the detection technique depends on the network density. Threshold that is considered for wormhole detection also depends on the network density. For the true detection of wormhole, proposed technique compares the hop count with the threshold. So the threshold is an important factor of simulation. If the value of threshold small than the hop count, it will give a higher value of false negative rate (that means it give true alternative route as a false route) and if the value of threshold is higher than the hop count, it will give false positive rate (that means it give higher alternative route as a true route). In the simulation, first the value of threshold is set one and then the results of the proposed algorithm are calculated. After that, the value of threshold is set two, and the result is again calculated and so on. The simulation of these scenarios shows that increasing the value of threshold the detection ratio of wormhole shows good result. The experiment is run over 100 nodes and it shows the positive result of wormhole detection. In the scenario the value of threshold is decided seven. The simulation shows the true path from source to destination before attack. On 25ms the attacker wormhole is activated and it creates a tunnel. The resultant path after the attack is shown in the figure 2 is shorter than the actual path, so the packet will take that path. For detection of wormhole attack in that path, the algorithm run to find an alternative path to the two hop neighbor node. If the hop count of that path is greater than the threshold this path will consider as a wormhole path. the path is S->1->2->3->4->5->6->7->8->9->D. After 25 ms the wormhole nodes that reside in the network perform attack and give the shortest path to the source node, because it is the properties of wormhole that it gives the shortest path to the source by providing the tunnel between two nodes in the path. So after the attack on that path the source node take another shortest path that have wormhole is S->1->2->8->9->D. In this path the source node assume that this is the shortest path and legal path between source and destination. The figure 2 shows that the wormhole node make tunnel between the node 2 and node 8, but the AODV could not detect the tunnel. It is clarify that the proposed technique is detect wither shortest path given by AODV having wormhole or not and it will help network administrator for taking the decision wither selected path is legal or not.

From the above consideration of threshold, simulation of proposed technique is compared with the existing AODV. From the analysis we see that the overhead of our technique is more compared to the existing AODV as show in figure 5.10. A graph of control packet is also shown, because the number of control packets in the proposed technique has increased. In the figure 7, it is shown that when the number of nodes increases the routing load is also increases. In the second scenario the simulation will be done with 72 nodes with same assumptions. After that, we take same scenario with 84, 100 and 200 nodes.

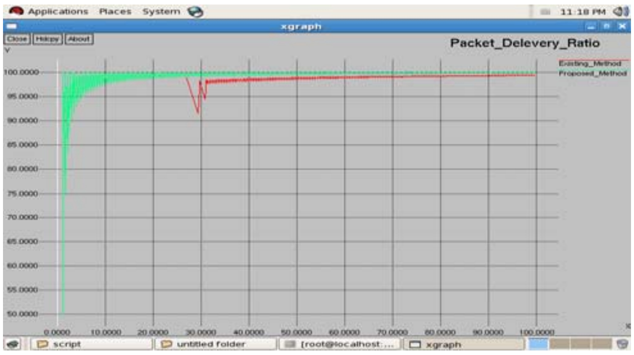

Figure 7;-Packet Delivery Ratio

We also analysis the ratio of packet send and receive rate of both proposed and existing technique as shows in Figure 5.10

Energy consumption: - In proposed beacon & neighbor node mechanism wormhole recognition is perform over that path suggested by AODV over P-2 node if path having P hop distance. As per describe in distributed approach every intermediate hop required two joule for sending control packet via detecting wormhole. Distributed approach required additional one joule energy by every beacon node for sending and receiving their GPS coordinate. So total energy use to detect wormhole via distributed approach in worst case is O(P*3)joule.

Whereas proposed beacon & neighbor node concept only P-2 hop play a role to detect wormhole along with that there is not any requirement to use GPS system. So total energy required to detect wormhole in worst case is O(P-2*2)joule .

Mitigation Percentage:- The above observation shows that the detection technique works efficiently but having some overhead, control packet as mitigation percentage is also increases in the graph, but the benefit of this technique is that it detects the wormhole, and will serve as an advantage when added to the existing AODV protocol. Figure 5.13 shows the result of mitigation percentage and it shows that when the number of nodes increases the value of mitigation percentage also being increases.

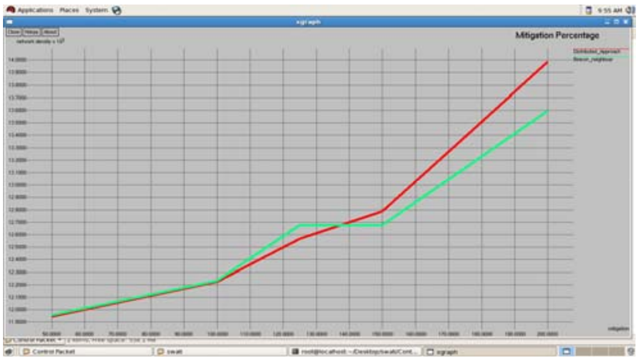

Figure 8:-Comparison Of Mitigation Percentile Between Distributed And Beacon Neighbor Node Concept.

IX. CONCLUSIONS

The wormhole is a major problem in the field of wireless network. To take this problem as a challenge this work has proposed an approach to detect and prevent the wormhole attack from the network. This is some kind of defensive mechanism. This is beacon neighbor node approach to defense wormholes in mobile ad-hoc network. The approach uses the two methods having their own limitation. This work uses the positive points of these approached and combined it. The performance of proposed technique is depending upon network density, having lower FNR ratio with network having larger number of node. Along with that proposed technique required lower power backup for wormhole detection along with that its required lower mitigation percentile and higher packet send and receive ratio as compare to existing one.

In order to detect wormhole proposed technique use larger number of control packet in future we will try negotiates that effect.

REFERENCES

[1] Maulik, R. ; Chaki, N., "A comprehensive review on wormhole attacks in MANET" IEEE 2010, Page 233-238.

[2] Jian Yin, Sanjay Madria, "A hierarchical secure routing protocol against black hole attack in sensor networks", IEEE SUTC, 2006.

[3] Xiangyang Li “Wireless Ad Hoc and Sensor Networks: Theory and Applications” Cambridge University Press 978-0-521-86523-4

[4] Sebastian Terence J , "Secure Route Discovery against Wormhole Attack in Sensor Networks using Mobile Agents", IEEE 2011, pp 110-115.

[5] C. Perkins, E. Belding-Royer, “Ad hoc On-Demand Distance Vector (AODV) Routing,” The Internet Society 2003.

[6] Sang-min Lee, Keecheon Kim “An Effective Path Recovery Mechanism for AODV Using Candidate Node” springerlink, vol. 4331/2006, 2006.

[7] Mahajan, V. ; Natu, M. ; Sethi, A. , "Analysis of wormhole intrusion attacks in MANETS", IEEE 2008, Page 1-7.

[8] Keer, S. ; Suryavanshi, A., "To prevent wormhole attacks using wireless protocol in MANET" IEEE 2010, Page 159-163.

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A secure routing protocol for ad hoc networks,” in Proc. of IEEE ICNP, 2002.

[10] Dang Quan Nguyen ; Lamont, L., "A Simple and Efficient Detection of Wormhole Attacks", IEEE 2008, Page 1-5.

[11] Katrin Hoeper, Guang Gong, “Pre-Authentication and Authentication Models in Ad Hoc Networks,” Signals and Communication Technology, pp. 65-82, 2007.

[12] Kanika Lakhani, Himani bathla, Rajesh Yadav “A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET” IJCSNS International Journal of Computer Science and Network Security, vol. 10 No.5, May 2010.