ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 7, Issue 3, March 2018

SECURITY MECHANISM IN MOBILE ADHOC NETWORKS AND PERFORMANCE EVALUATION OF HETROGENEOUS ADHOC NETWORK

Tabrez Hussain[1] (tabrez.hussain1@gmail.com)

Sanya Tandon[2] (sanyatandon112@gmail.com)

Vibhor Sharma[3]Himanshu Khanna[4]

Maharaja agrasen institute of technology Delhi

ABSTRACT

A security issue of cooperative immunization compared to collaborative attacks such as the black-hole attacks and the wormhole attacks in a real heterogeneous mobile ad hoc network was discussed. A temporary assembly of wireless mobile nodes in distributed manner is known as Heterogeneous Ad hoc Network (HANET). In a hostile environment of HANET, security is the primary concern to accomplish protected communication between mobile nodes. A number of nontrivial experiments to security designs order the demand of building multi-fence security solutions that achieve both extended protection and adorable network performance. HANET's are susceptible to numerous security attacks because of shared channel, insecure operating situation, lack of central authority, incomplete resource availability, and dynamicallymutable network topology and resource constraints. Wormhole attack and Black-hole attack are different network layer attacks and wormhole is the dominant attack of all. In this work, wormhole attack and Black hole attacks are implemented. Black hole attack is the denial of service attack. Many algorithms had been proposed to prevent this attack.

Keywords:HANET, wormhole attack, Black hole attacks etc.

I. INTRODUCTION

An ad-hoc network is a combination of more than two devices equipped with wireless communications

and capabilities of networking. It allows anywhere, anytime computing. This setup is adaptive and self-organizing. It supports both peer-topeer communication and peer-to-remote communication.

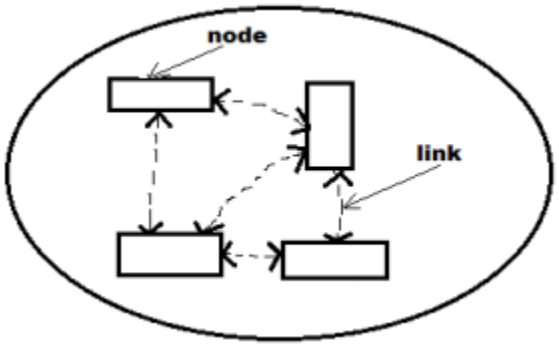

Figure 1: Architecture of Ad-hoc network diagram

An Ad hoc network can be divided into homogeneous network (all devices are identical, have same features and capabilities) and heterogeneous network (neither devices are identical nor have same capabilities) on the basis of nodes. As if all mobiles or computers like nodes are connected, then network is homogenous otherwise heterogeneous.

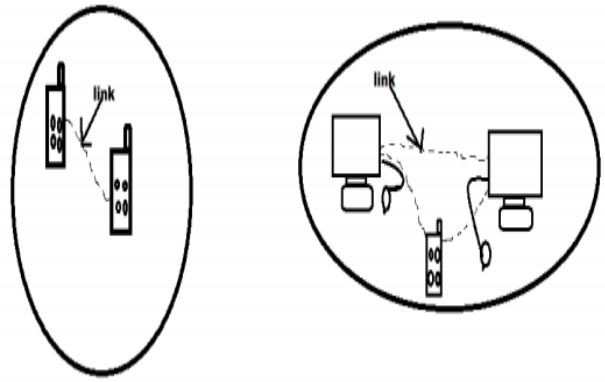

Figure 2: Homogeneous and Heterogeneous ad-hoc network

Modelling a Heterogeneous Attack against Ad-hoc Routing Protocols:

This section mainly addresses the Heterogeneous Network, which may cause more devastating impacts on ad-hoc networks than single and uncoordinated

attacks. In general, the heterogeneous attack model was developed to investigate the weaknesses of the routing protocols of mobile ad hoc network that exploits the vulnerabilities of ad-hoc environments, which will harm the system and results in a vulnerability assessment. This Heterogeneous Attack makes use of the combined effort of more than one attacker against the target victim. Moreover, this attack may launch multiple intruders to synchronize their activities and accomplish the usurpation, deception, distribution destruction, modification of data, and disclosure against targeted routing protocols to deny the service to legitimate nodes and completely terminate all activity to the network entities.

Wormhole Attack

It is a network layer attack. In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

BLACKHOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route requestand thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

II. LITRATURE REVIEW

Wormhole attack is the one of the major network layer attack of MANETs. In order to deduce the best suited protocol for wormhole attacked network, researchers employed detailed analysis of different protocol categories with varying the various simulation parameters. This section presents the existing background and related work of analysis of various protocols under wormhole attack in MANETs.

AnujRaiet. al. [1] have proposed a novel way of detecting a black hole node in the network by using Trap RREQ messages. The method involves sending a trap route request message, before sending an actual route request. Sender's of all the reply messages are blacklisted as malicious nodes. This approach introduces a significant amount of delay, and it doesn't address the co-operative black hole attack.

NabarunChatterjee [2] et. al. suggested a method involving encryption to avoid black hole node during the path setup phase. Sender node sends some plain text to the destination node with the route request message, and the destination node sends the encrypted text with the reply message. This method allows only destination node to respond to route request; thus this method is not scalable.

Saravanamet.al [6] evaluated and analyzed the reactive protocols (AODV, DSR) and proactive protocol (OLSR) with different methods and trajectories using OPNET 16.0 to found the best protocol for wireless networks and revealed that reactive protocols has efficient output as compared to proactive protocols in high mobility networks for heavy load because of new path discovery and path maintenance.

Jenny et.al [7] analyzed the impact of wormhole attack on AODV, DSR and Fisheye protocols in mobile and unmobileadhoc networks and found that DSR protocol performs better in terms of packet delivery ratio and throughput but end to end delay is very large when compared to other two protocols in a wormhole attacked network.

Sundararajanet.al [8] tested performance of seven different routing protocols (AODV, DSR, ANODR, DYMO, OLSR, OSPF, LANMAR) in variable network sizes with and without wormhole attack. The performances of all protocols were decreased because huge amount of system resources and processing power needed when network size increases. In homogeneous networks among on demand routing protocols DYMO protocol performs 21.5% well. Among other protocols LANMAR protocol performs 12.9% well. In heterogeneous networks among on demand routing protocols, DYMO protocol performs about 18.4% well. Among other protocols LANMAR protocol is performing 9.4% well. When there is an attack overall performance reduced about 20.1%.The packet delivery ratio in homogeneous network was 33% greater than homogeneous networks because in

homogeneous network there is no different devices, no different frequencies and no different interfaces needed hence packet delivery ratio is more. The average end to end delay in heterogeneous network is greater than homogeneous network by 8%.

Aroraet.al [9] analyzed the AODV and DSR Protocol with wormhole attack in wireless mesh networks by varying the node mobility speed and revealed that for protocols, throughput decreases and average end-to end delay increases in the presence of wormhole nodes as compared to absence of wormhole nodes.

III. Problem Statement

In this section, we present the wormhole and Black hole attack model and illustrate how a wormhole attack and Black hole can significantly impact the performance of network protocols, such as routing, and applications of mobile ad hoc networks, such as monitoring. We then abstract the problem using graph theory and provide the necessary and sufficient conditions to prevent the wormhole and Black hole attack. Throughout the rest of the paper, we will use the terms wormhole attack and Black hole problem interchangeably to refer to a network with wormhole links.

IV. PROPOSED METHOD

In proposed work, firstly we deploy the mobile ad hoc network with 100numbers of mobile nodes. All the mobile nodes are randomly deployed into the fixed area. The source and destination are selected for route establishment. For the route establishment source node flood the route request packet in the network and route reply packets are send back to the source by the adjacent nodes. The route is established between source and destination on the basis of hop counts and sequence numbers. The malicious node exists in the route which is selected between source and destination. The malicious node will be responsible for triggering the selective packet drop attack. The proposed mythology will detect the malicious node and isolate, it from the network. The methodology is based on the throughput, Average energy and Delay of the network. When the throughput, Average energy and Delay of the network, will degrades to certain threshold value, nodes in the network will go to monitor mode and detect the malicious node. The proposed methodology will be implemented in MATLAB 2014a.

We consider HANETs which consists of mobile nodes and attackers. All nodes are heterogeneous, symmetric and dynamic in nature. We assume that communication channels uses bidirectional mode; it means node A accept message from B then B can also accept message from A. To establish communication between two nodes normal wireless transmission range is used. We assume that two wormhole nodes are connected with each other using high speed link known as out-of-band channel. This long range channel is called wormhole link and two end points used are known as wormhole nodes. Our consideration is to detect wormhole link with larger delay. The proposed work is based on the details of following assumptions:

1. All the nodes are communicating in the same environment and are having the same communication range.

2. The source node cannot be used as a wormhole. It can never cause wormhole attack in the network.

3. While calculating maximum end to end delay; we are considering processing time of the packet, queue delay and packet loss as negligible.

Transmission Range

Friis equation is used to mark the presence of wormhole attack in the transmission range. Friis equation can be simplified; but factors like polarization, impedance, placement of antenna, reflection from building make this equation more typical and complex. The ideal condition where these factors cannot effect is satellite communication, where atmospheric factors are negligible [3, 4]. When the source node broadcast a packet, it won't be able to communicate beyond a certain range. The formula to calculate communication range for distance'd' is as follow in (Eq. 1):

$$\frac{P_r}{P_t} = G_t(\theta_t,\phi_t)G_r(\theta_r,\phi_r)\left(\frac{\lambda}{4\pi R}\right)^2\left(1-|\Gamma_t|^2\right)\left(1-|\Gamma_r|^2\right)|V_t.V_r*|^2 c^{-\alpha R} \quad \textbf{(1)}$$

Where as, G_t and G_r are the gains of transmitting and receiving antennas. (θ_t,ϕ_t) and (θ_r,ϕ_r) direction of transmitting and receiving antenna. Γ_t and Γ_R reflection coefficients gains of transmitting and receiving antennas. V_t and V_r are polarization vectors. -α is absorption coefficient of medium. R is distance between receiving and transmitting antenna.

Attack Detection

In this section, we described our proposed wormhole detection and Black hole technique in detail. Attempt is to detect suspected link which is part of a wormhole. Then try to assure these links are not used for data transfer in future. We described our wormhole detection technique in AODV routing protocols.

The source node would undergo a process to discover route for destination, so it broadcast packet to all of its neighbors. Now, whenever any malicious node is intended to steal the data from the network, it would behave as an intermediate node and would falsely pretend to have a path to destination. Same happens in wormhole attack where the route is falsified by increasing the communication range and shortening hop counts of route by creating the tunnel.

Figure 3, shows an example of proposed wormhole detection technique.

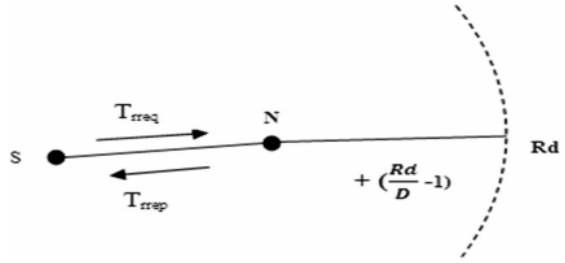

Figure 3: Wormhole Detection Technique. T_{rreq} = Time taken for route request to reach one hop neighbor, T_{rrep} = Time taken for reply packet to reach source, R_d = Communication range, D = Distance from source to neighbor, N = One hop neighbor

The step by step detail of our proposed scheme as follow:

1. The source node will send the route request to the nodes in its communication range. These will be referred as one hop nodes.

2. The source node can never cause the wormhole attack in the network, taking this forward time difference will be calculated.

3. After receiving the RREQ, the one hop nodes will inform the source node about the time when the packet was received. After having the knowledge of the packet received time, the source node can know about the complete time taken to communicate with one hop node.

4. The source node will calculate the threshold for the maximum delay which can occur between the two nodes.

5. A source node can have more than one neighbor nodes. The source node will compute the time difference (time when it sent the RREQ packet and time when the node received it). Say the maximum time difference value obtained is T.

6. Now threshold formula will be (Eq. 2):

$$T_{rreq} + T_{rrep} + 2 * (T * ((Rd/D) - 1))) \quad \textbf{(2)}$$

whereas, T_{rreq} is the time taken by the packet to reach the node during route request phase. T_{rrep} is the time taken by the packet to reach the source node when its neighbors reply back. Rd = Node's communication range. T = End to End delay between source and its one hop neighbor. D = Distance between the source and the neighbor for which T is calculated.

$$D = \sqrt{(X1 - X2)^2 + (Y1 - Y2)^2} \quad \textbf{(3)}$$

(whereas, X1, Y1 are coordinators of source. X2, Y2 are coordinators of neighbor nodes.)

7. T_{rreq} + T_{rrep} will total communication time between the nodes. And additional factor is added to account for the remaining distance w.r.t. the communication range.

8. This will give us the maximum value of delay which can occur between the two nodes while forwarding the RREQ message towards the destination node and sending RREP message back to the source node. By assuming the path loss negligible and then any node should not take time more than this value to communicate.

9. The source node will store the threshold value.

10. The one hop nodes and the subsequent intermediate nodes will forward route request packet towards the destination along with the time at which request was received by them from the predecessor nodes.

11. When the RREQ packet will reach the destination node, the destination node will start the route reply phase.

12. The nodes which occur in the path from source to destination must send the time at which reply message was received by them.

13. The source node upon receiving the reply messages from various paths will compare the timings of every hop with the threshold value.

14. If the time difference between two nodes is greater than the threshold value, then the wormhole link will be detected by the source node.

15. The source node will not select the path having the wormhole links and will send data to the destination node via other path.

V.RESULT

In this segment, we conducted the simulation to measure the effectiveness of proposed scheme with following network configuration setup using MATLAB 2014a: 100 mobile nodes with in the area of X=100, Y=100. The transmission range for the number of round is 100 with random way point mobility model. We position the malicious nodes randomly within the network to perform the wormhole and Black hole attack. The results are summarized as follow in Table 1

Table 1: Input Parameter

Input parameter	Value
Number of Nodes in the field	100
Xm	100
Ym	100
P	0.1
Eo	0.2
ETX	50*0.000000001
ERX	50*0.000000001
Efs	10*0.000000000001
Emp	0.0013*0.000000000001
EDA	5*0.000000001
No of rounds	100
Packet size	40

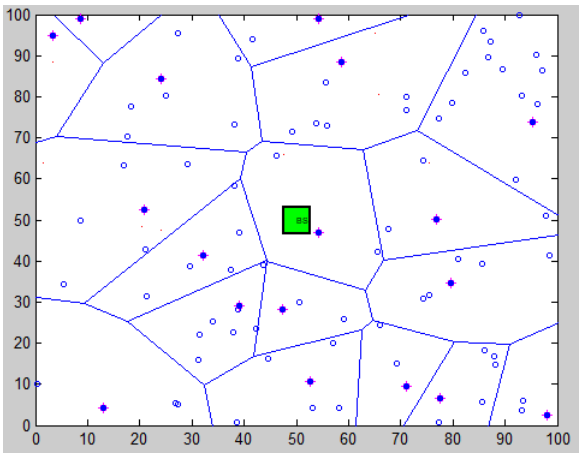

Figure 4: Network simulation

In 100 runs of simulation scenario with the malicious environment simulation results shows that network life is decreases as the number of random round is increased.

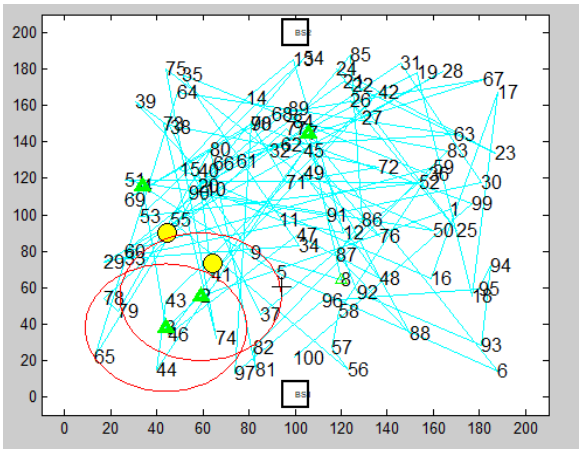

Figure 5: Network communication normal to advance node

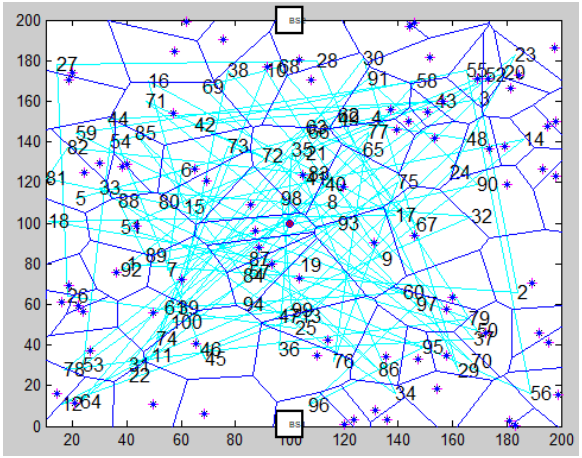

Figure 6: After execution of work

(a) Average Energy of Each round

Average Energy is made up of two parts; control overhead and packet overhead. Control overhead is the fraction of bits in control packets over bits in data packets. Here, the average energy is characterized by the total number of bits transmitted per successfully delivered data bit

$$\mathrm{OH} = \frac{B_{\mathrm{tx}}}{L_{\mathrm{data}} \cdot N_{\mathrm{p}} \cdot \mathrm{PDR}} \quad (4)$$

Where B_{tx} is the total number of bits transmitted. B_{tx} is given by

$$B_{\mathrm{tx}} = N_{\mathrm{f}} \cdot N_{\mathrm{p}} \cdot L_{\mathrm{p}} \quad (5)$$

Where, N_f is the number of forwarding neighbors.

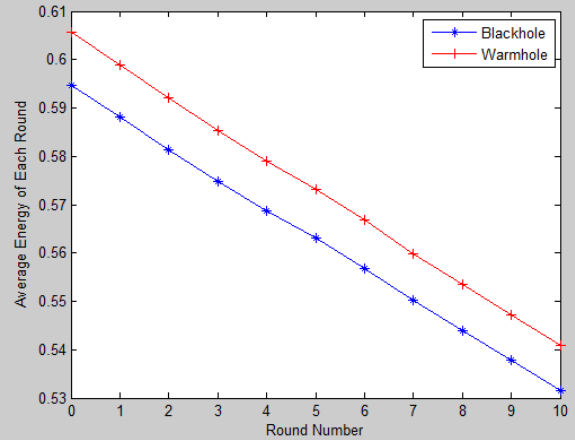

Figure 7: Average Energy of each round on 10 round numbers

As shown in above figure the average energy of Black hole is less than the Worm-hole attack.

(b) Throughput

The throughput, TP, is defined here as the number of data bits successfully delivered to the sink, per second. This is expressed as

$$\mathrm{TP} = \frac{L_{\mathrm{data}} \cdot N_{\mathrm{p}} \cdot \mathrm{PDR}}{T_{\mathrm{t}}} \quad (6)$$

Where,N_p is the total number of packets produced and T_t is the total deployment time of the network. The expression shows how the throughput is largely affected by the number of packets generated and the number of packets lost.

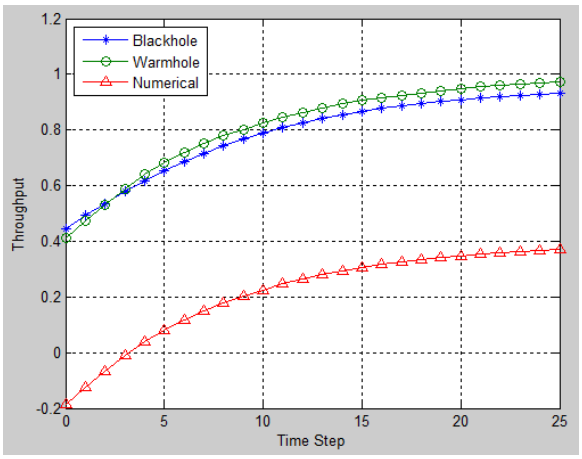

Figure 8: Throughput of the Black-hole, Wormhole and Numerical in Time step

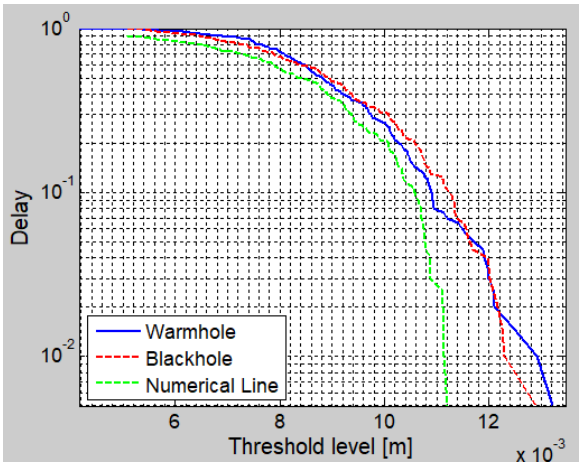

Figure 9: Average delay Black-hole, Wormhole and Numerical on Threshold

(c) Average end-to-end delay

The average end-to-end D_{av}delay is defined as the average time between a node creating a packet and it being received at the sink. Given as

$$D_{\mathrm{av}} = h \cdot T_q. \quad (7)$$

Where h is the number of hops and Tq is the delay at each node. The average hop-count between the source and the sink is taken from

$$h = \frac{d_{\mathrm{av}}}{d_{\mathrm{hop}}} = \frac{2 \cdot L}{3 \cdot r \cdot \cos\left(\pi/2 \cdot N_{\mathrm{n}}\right)} \quad (8)$$

Where dav is the average Euclidean distance between the source and destination, and d_{hop} is the average distance of a single hop. L is the length of the square network area, r is the node's transmission radius and N_n is the expected number of neighbors to each node. N_n is given by

$$N_n = \left(\frac{\pi \cdot r^2}{L^2}\right) \cdot (n-1). \quad (9)$$

Where n is the total number of nodes in the network. The arrival rate of packets to a node, l, is assumed to follow a Poisson distribution and each node is considered to be a single server. Since the global TDMA has a deterministic medium access time, the service time, Ts, is constant. For this reason each node is modeled as an M/D/1 FCFS queue. In each node packets are created at a rate of fp. The total number of packets forwarded by a node is equal to the packet creation rate multiplied by the number of nodes, whose data it forwards

$$\lambda = \frac{f_p \cdot (n-1)}{N_n^2} \quad (10)$$

As each node gets the chance to transmit once in a TDMA cycle, the service time is simply

$$T_s = \Delta \cdot (n-1) \quad (11)$$

Where Δ is the length of a single time slot, which is given by

$$\Delta = \frac{L_p}{R_b} + \frac{r}{c} \quad (12)$$

Where R_b is the bit rate and c is the propagation velocity of the signal. Using the Pollaczek–Khinchin formula for the mean time in the system, Tq, the delay can be described as:

$$D_{av} = \frac{h \cdot T_s \cdot (2 - \lambda T_s)}{2 \cdot (1 - \lambda T_s)}. \quad (13)$$

This expression highlights the contribution of the number of hops and packet arrival rate to the delay time.

V.CONCLUSION

In this paper, first we have made a performance comparison of three different mobile ad-hoc routing parameters with respect to various network sizes in heterogeneous network. In the next level, we test the performance of same protocols in the presence of attacking nodes. In previous works performance of routing protocols were evaluated as function of mobility rate and speed without considering the network size. However Scalability is a very important factor in some applications of mobile ad-hoc networks, as it determines if a protocol will function or fail when the number of mobile users increases. We used MATLAB 2014a simulator, which is commercial and said to be faster than ns-2 for instance. However, the simulation speed is still slow and we were only able to perform a single run per scenario in the context of this research. Therefore, those results should be validated through multiple, additional simulation runs in a future work.

REFERANCES

[1] AnujRai, Rajeev Patel, RK Kapoor, and DS Karaulia. Enhancement in security of aodv protocol against black-hole attack in manet. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, page 91. ACM, 2014.

[2] NabarunChatterjee and Jyotsna Kumar Mandal.Detection of blackholebehaviour using triangular encryption in ns2.Procedia Technology, 10:524–529, 2013.

[3] Atmel. Range calculation for 300 MHz to 1000 MHz communication systems. http://www.Atmel.com/Images/doc9144.pdf. February 16th, 2012.

[4]https://en.wikipedia.org/wiki/Friis_transmission_equation.

[5] OMKAR Pattnaik, SasmitaPani(2012), Application of IDS in WSN: a survey , IJRCCT, 7, 1

[6] V. Saravanam, D. Vijayakumar, "Performance of Reactive and proactive MANET Routing Protocols With different Trajectories", International Journal of Engineering Research & Technology (IJERT), Vol. 1Issue 8, October2012

[7] R.Sherine Jenny, N.Sugirtham, "Simulation Based Performance Comparison of AODV, DSR, FSR Routing Protocol with wormhole attack",IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.3, No1, February 2013.

[8] T.V.P. Sundararajan ,Karthik , A. Shanmugam, "Security and Scalability of MANET Routing Protocols in Homogeneous & Heterogeneous Networks", Proceedings of the International Conference on Man-Machine Systems (ICoMMS),11 – 13 October 2009, BatuFerringhi, Penang, MALAYSIA

[9] Mani Arora, Rama Krishna Challa, DivyaBansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology (ICCCNT), DOI 10.1109/ICCNT.2010.34 , IEEE, 2010