REVIEW OF BLACK HOLE AND GREY HOLE ATTACK

Rupinder Kaur[1] and Parminder Singh[2]

[1]Student, IT Deptt, CEC, Landran, Mohali, India
[2]Assit.Professor, IT Deptt, CEC, Landran, Mohali, India

ABSTRACT

Black hole and Grey hole attack is most happening attacks in Mesh networks. Mesh networks means non-static networks with making loops of networks with the help of active hotspots. In Wireless networks all the communication between the nodes is happening wirelessly and the nodes are so much resource constraint that it is difficult to employ any security solutions of other ad hoc networks. So they are attacked by malicious nodes. In black hole attack the attacker windup all the information and dropped it.

In black hole attack, the series of RREQ (route request) and RREP (route reply) follows the smallest way of networking communication. The fault node always transmit RREP message as it receives RREQ, while managing the receivers sequence number. By the help of fault node packets are dropped. Sometimes fault node is authorised and otherwise it is unauthorised. Black hole attack is type of routing attack and can bring harm to whole network. Grey hole attack is the kind of denial of service attack. In this attack, the router which is mesh behave just not well and a subset of packets are forward and handle by receiver but leave by others. The presences of these attackers are hard to detect in wireless networks because over the wireless link the packets are lost due to bad channel quality. This paper deals with the study of analysis of delay occurs by these attack in Wireless Mesh networks and its types and also discuss about previous study by which we get idea about attack occurs in networks and also study various techniques to detect and prevent network from black hole and grey hole attack. Then we discuss about their result by using simulator OPNET.

KEYWORDS

Black hole attack, Grey hole attack, MRP, OLSR, RREQ, RREP, RERR, OPNET.

1. INTRODUCTION

Wireless mesh networks (WMNs) are becoming famous now-a-days in different areas like military applications, environment application etc. Wireless Mesh networks is a virtual network which makes connection virtually or wirelessly in network and that connection is made with network nodes or hops. In wireless mesh networks nodes are movable. As a result, many attacks occur by attacker on virtual mesh networks. Black hole attack is an ancient attack of virtual mesh network which held on routing layer. Black hole attack brings major effect on network.

The user can analyse the results in base station where any physical mechanical change in environment are send by nodes of WMN. Suddenly the topologies of network can changes without reason. There is limitation in support system where each node play role like router and different node connect anywhere and diffuse the network at any time. Wireless mesh network is type of dynamic network structures. WMN have many disadvantages on resources like memory, processing power and power of battery. In different way, an object in classical wireless LAN ,all nodes are movable and changes in topology is done suddenly in wireless mesh network, which is difficult job to hold the security of wireless network. As a result, attacker joins the network and takes packets and rejects the network. We reduce the communication cost of nodes by performing signal processing, computation of local data to base station. Black hole and Grey hole attacks are the two classical attacks under wireless mesh network, which destroy the network topology and decreases the network performance.

In this paper, we discuss how malicious or false node delay in network when black hole and grey hole attack occurs. To understand the behaviour of these attacks, we must secure the wireless network from these attacks. In order to gain this, we scattered and similitude the behaviour of attacks in description. We have done all the simulation using OPNET 14.5.

1.1 BLACK AND GREY HOLE ATTACK

Black hole attack is a routing layer attack in which data is revolves from other node. The transmission of packets on multiple nodes and dropping of packets is mostly occurring on routing layer. Routing protocol is targeted by the attack. Black hole attack having great influencing attack on virtual mesh network. The busy DOS attack is black hole attack. Black hole attack is difficult to detect; it is mostly found in temporary networks like virtual/wireless mesh networks.

Black hole attack will cause powerful effect to the performance of mesh networks. In previous research, the authors have carried out on black hole attack [6].

In black hole attack, the sender node receive reply message from fault node and make smallest way to receiver node. Fault node sends reply message after authorised node to sender node and then sender become confuse in two replies. On that way, Fault node become sender node and whole data received by it. In this, the data packets fully dropped by sender node.

In Figure 1, the sender node 1 sends large amount of RREQ message to every nearby nodes. When RREQ message is received by fault node, then it sends RREP message to sender node which is non-real and also shows the shortest way to reach to receiver node.

Then sender node accepts the reply message from non-real node which is called fault node and transfers the packets. This attack is known as black hole attack.

In black hole attack, a fault node accepted by sender node not attention and all the data packets are dropped. This is also known as sleep derivation attack. This attack is divided into two types, i.e. Internal and External black hole attack. We explain these attacks as follows:

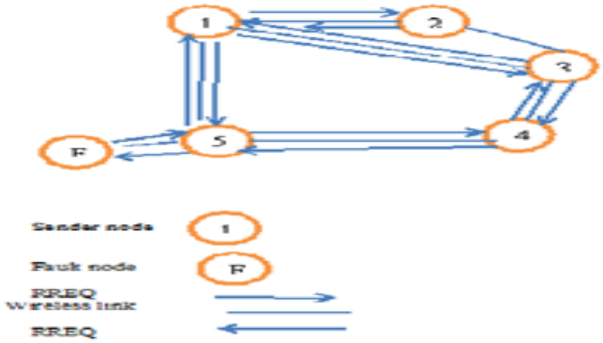

Figure 1: Black Hole Attack Specification

(a) Internal black hole attack

It occurs in network internally. it means the internal node is become the fault node and makes route from sender node to receiver node.

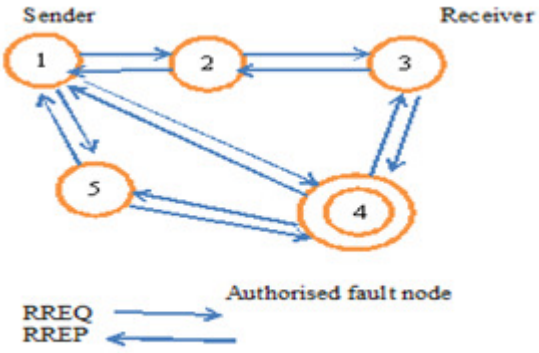

Figure2: Internal black hole attack

In Figure 2, the sender node 1 sends RREQ to each node and gets reply back from every node; the whole network is set up by authorized nodes. Suddenly, the authorized node becomes fault node and internal black hole attack occurs.

(b) External black hole attack

This attack occurs outside from the network. It is mainly called DOS (denial of service) attack.in this attack, network take advantage from network traffic and collapse the whole network. It is done by External fault node and then working as same as internal node. It follows some steps which is given below:

1. Fault node become active node and makes way to receiver node.
2. Fault node send RREP message and shows the smallest way to receiver node and become part of network.
3. It receives all the data packets from sender node which is transmit in network.

4. The series of RREQ and RREP message occur and data transfer is done and black hole attack occurs.
5. The data is receiving the fault node and 100% packets are dropped in network.

The black hole and Grey hole attack will carry a large price of effect to the performance of wireless mesh network. In multiple ways the false behaviour may exhibits by Grey hole attack, Grey hole attack is a node which react maliciously for some specific time duration by releasing packets but may come to balanced behaviour and later forward the packets through packet ID to other packet. A Grey hole may also behave a random behaviour by which it rejects some the packets randomly when it forward to other packets. Thereby its detection is even more difficult than black hole attack.

2. RELATED WORK

Karof et al [3] was the first person who explain the different kinds of vulnerabilities in wireless mesh network. They found that there are many attacks like Sybil attack, HELLO FLOOD attack along with black hole and grey hole attack which is possible in wireless sensor networks. Many other researchers have also stated that the normal routing process can easily disrupt by malicious node which is deploy by security techniques.

Richa et al [19] have only nominate the detection but also find out the removal of adversaries' by middle node through packets. It is the best method we have study the impact of black hole and grey hole attack in different sizes in wireless sensor network.

Damandeep et al [7] proposed that the promiscures node method to detect the malicious node in worm hole attack by using routing protocol AODV. The alarm message is generated when delay in network occurs.

Satoshi et al [21] analysed the black hole attack and explain a route from malicious node must increase the destination sequence number for particular purpose to decide the source node. Authors analysis and propose a statistical base anomaly detection approach to detect the black hole attack and on destination side they received RREPs (Route Replys) according to destination sequence number.

3. OLSR ROUTING PROTOCOL

The optimized link state routing protocol (OLSR) given in RFC3626, which is designed in mesh network. OLSR is proactive routing protocol: the information is route, when they needed. It is also called table driven protocol. The updated topology of the network is maintained by this protocol. In this each node in network is known by every node before a particular time. All the direction information is stored in tables. Whenever network topology becomes different, these tables are come with new information.

OLSR spread the network of particular facts by large amount of packets in every part of network. The large amount of flow of packet is done on each and every node that received packets are broadcast again. These packets contain in a correct order so as to stay away from making the curved shape with network. The receiver node put the information in correct order, making

without any doubt that those packet broadcast one time. OLSR has three kinds of impose messages which are discussed as follows:

1. HELLO: This impose message is broadcast an ability to understand the nearer node and Multi-Point Distribution Repays (MPR) judgments.
2. TOPOLOGY CONTROL (TC): By the help of OLSR signaling is performed link state information is optimized by the used of MPRs.
3. Multiple Interface Declaration (MID):This message contain every IP addresses that has already been put to the purpose to intended by the smallest number of node in network. All the nodes in OLSR broadcast the message on more than one connection.

The starting point of MPR is to degrade the exact copy or the curved shaped of network broadcast again the packets. Route packets are broadcast by only MPR nodes. The authorized nodes in the network managed a record of MPR nodes.

MPR are choose with in the immediately area of sender node. The choice of MPR is mainly forced on HELLO message or RREQ message which transmits into the nearer node. The choice of MPR is the way to be real to every of its nearer joints through MPR nodes. Routers are accepted one sender node that's need to start broadcast the sending data packets.

In OLSR black hole attack the fault node "F" is found the busy route into the sender node "S" and receiver node "R''. The fault node "F" then transmits the RREP which makes correct order to node "T". This node "T" towards the RREP to the sender node "S". This route is transfer packets to fault node. These packets are dropped. In this way, sender and receiver node are not communicate in condition of black hole attack.

The fault node chooses to drop RREQ and RREP message packets. In this, the unwanted node drops packets by sending non-real RREP to sender node.

In Figure 3, node F which is fault node can make illegal copy of RREP message to sender node S. When sender node S receives non-real RREP messages from node F, it updates information in tables of route to the receiver node. When node F accepts the data packets it dropped the packets as shown as follows:

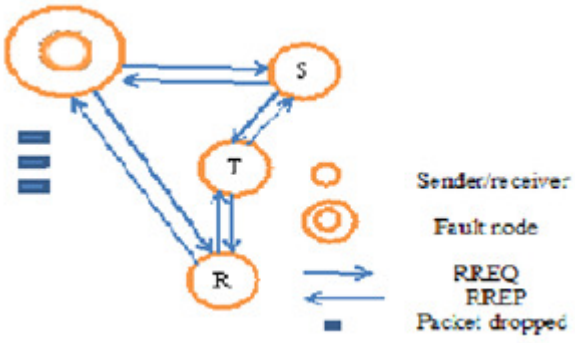

Fig 3: Dropping of packet in black hole attack

A black hole attack has two qualities:

1. The node used the virtual routing protocol and known publically itself making reasonable route to receiver, even the route is non-real with the plan to stop packets.
2. The node used to stop packets. The fault node always transmits RREP as it receives RREQ, while managing the receiver correct order. The RREP transmit by the fault node is behaved as new. Thus, fault nodes achieved in black hole attack.

4. PROPOSED WORK

Black hole and Grey hole attack is a major Question in wireless mesh network. Our proposal is based on the analysing these attacks in 802.11b network environment and calculate is delay in both attack, that how black hole and Grey hole node effect the network delay. Its implement it by taking nodes as vector; i.e. one node is link with two nodes in x-axis and y-axis, and further make links as vector quantity.

In this each node is connected to next nodes and packets broadcast it. There is all mobile nodes, which is not fixed in position and all nodes are connected with one IP called backbone. Firstly, it's make scenario of wireless nodes and deploys random way point on each node and then change wireless LAN parameters. It's give each node as unique basic service station number and also set channel for these service station and then transfer the packets and generate graph of network without attacks. Secondly, after that Its change one node as false node and generate black hole then transfer the packets and generate graph. By this false node our packets shows source value but receiver node value is zero ,that means whole packets are dropped and at receiver node information is not adapted by receiver node .After this, we make that false node as Grey hole node, configure it by taking variable seeds and generate graph of that scenario. Finally, we configure this scenario by taking OLSR(optimized link state routing protocol) protocol in each statics then compare the performance. OLSR is also stored all the information in tables. It updates the topology of network which is changed in wireless mesh network. In network layer OLSR protocol accumulated throughput is calculated.

These all works has some advantages which are as follows:

1. In this, each node is connected to two nodes and all the information is stored in tables.
2. Its require no encryption on topology control, so information sharing is easy.
3. There is not necessary to watch all nodes, one node record link of just two nodes by which it link.

5. SIMULATION ENVIRONMENT

The term network delay is analyzed by performing the implementation of OPNET simulator. Simulation of black hole and Grey hole attack on the OPNET is achieved by having a false node. This node is detected Delay in simulation environment by using OLSR protocol in order to stop the behavior of false node.

In following scenario which is set of 30 mobile nodes. These mobile nodes are moving with constant speed of 10 m/s and simulation time taken as 1000 seconds. Area of simulation is taken

as 1500*1500 meters and mobility model is random way point with speed 10 m/s and transmitting power is by default 0.005 watts.

The random environment is chosen in wireless mesh network and other specification of simulation is as follows:
\

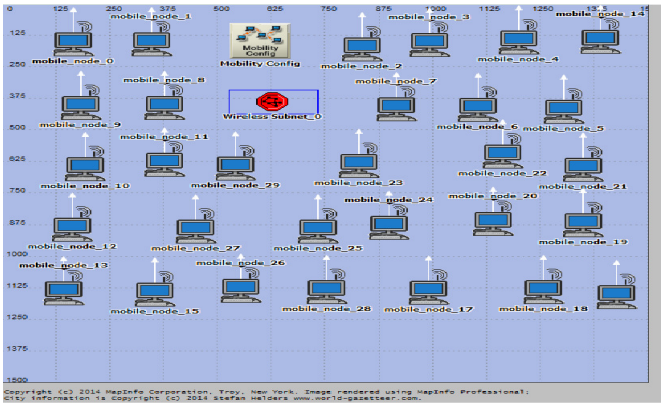

Figure 4. Scenario of 30 nodes

Figure 4, shows the scenario in which 30 wireless nodes are connected and communicate. Nodes communicate with the help of broadcast ip address ,i.e 192.168.5.63 .Our main goal is to check which attack is more dangerous effect on network performance .The last but not least stage and very vital of the time is given to this stage.

6. SIMULATION RESULTS

In random simulation environment, the first step is to determine the network delay on network performance with and without attack. Results are analysed carefully by obtaining from OPNET simulation. Its simulate a network of 30 mobile nodes. In OPNET there is set of two types of statics i.e. global and node. Initial take a uniform scenario with no black hole and grey hole attacks. There is no prevention is applied, then attacks will occurs. The false node is choose randomly in simulation test, and increases delay in network. The simulation results are presented in figure 5 ,figure 6and figure 7; which shows the network delay without attacks and with both attacks, i.e. black hole and Grey hole attack as follows:

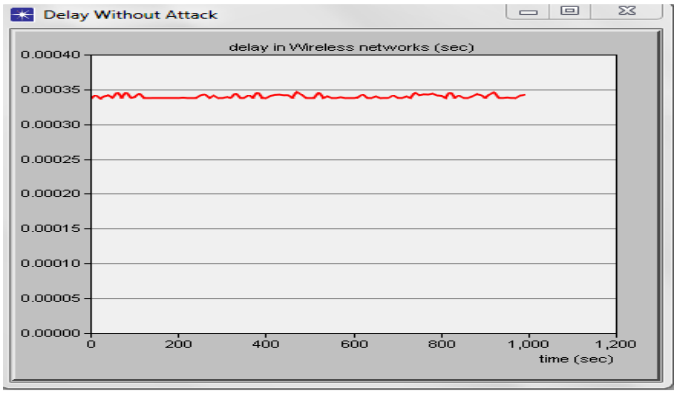

Fig 5: Network Delay in wireless LAN

Firstly, in without attack graph its transmits the packets in the form of bits from source to receiver node. After this Its originate one false node in network ,that false node is black hole or Grey hole node then delay in network occurs. That delay in network is signify the performance which shows as follows:

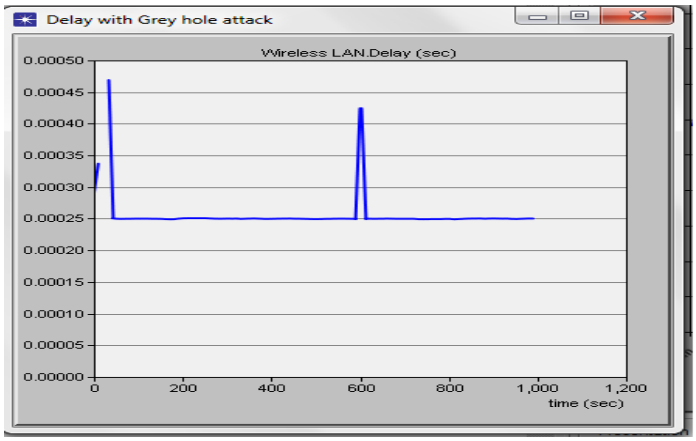

Fig 6: Delay with Grey hole attack

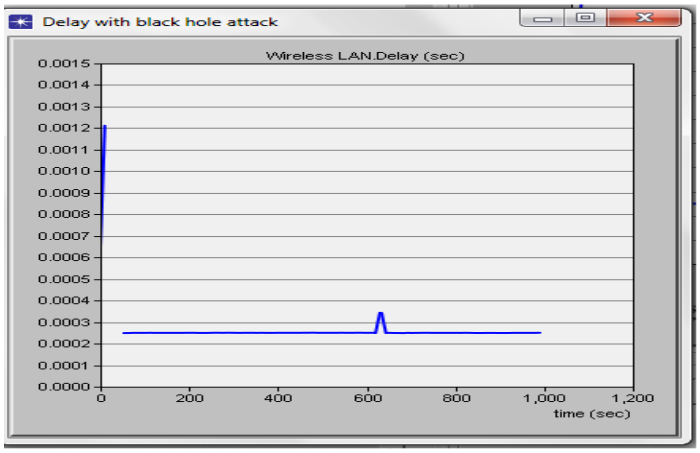

Figure 7: Delay with Black hole attack

After attacks, We Apply Secure path Scheme with OlSR protocol and found delay in network performance which is shown as follows:

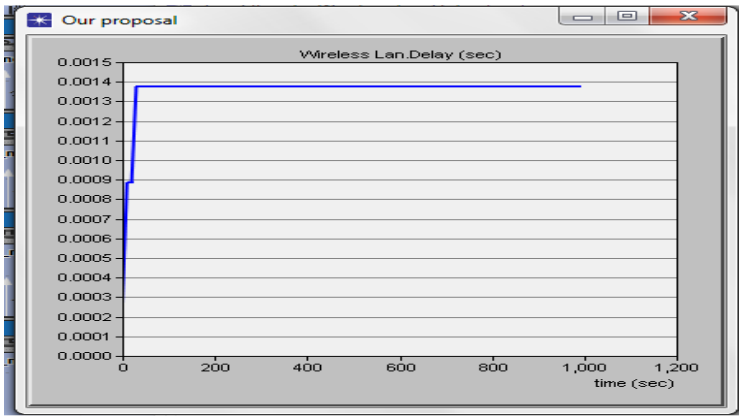

Figure 8: Delay with Apply OLSR protocol

7. CONCLUSION

The paper is usually attention with most important part of black hole attack in wireless/virtual mesh network such as how it is explained, divide according to their types and how it obtains in network to operate the fault activities usually of packet dropping. As a future scope of paper to share an attempt to examine several answer to this black hole attack and control the excellent in the middle of these.

The important feature in wireless mesh network is security. In this paper, the black hole and grey hole attack is come on network layer. due to movable nature, wireless mesh network have many weakness. Our aim is to prevent the network layer from these attack in which false node act as regular node. That node is difficult to detect, because the nodes here in this type of attack are very much unpredictable and volatile as they varies from normal to adversary and adversary to normal nodes. In this paper, Its apply OLSR protocol and find out that it stops some effect of these attacks, but Its cannot safe network from these attacks purely. It's also find that black hole attack is easy to detect than Grey hole attack. At performance level, there is not much difference in both attacks.

FUTURE SCOPE

There are number of attacks found in Network layer. If we need our information secure from attackers, then secure network layer must be provided. To study the related researches, its find how attack occur in network layer. Our main goal is to detect the black hole attack and Grey hole attack and find security better so that performance of network is not decreases.

REFERENCES

[1] A.Patcha, A.Mishra, "Collaborative Security architecture of black hole attack prevention in mobile ad hoc networks[C]",Radio and Wireless Conference,2003,pp.75-78

[2] B. Sun, Y. Guan, ,J. Chen ,U.W Pooch, "Detecting Black hole attack In Mobile Ad-hoc Netwoks[C]".5th Europeen Personel Mobile Communications Conference,2003,pp. 490-495.

[3] C. Karlof, D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures, Special Issue on Sensor Network Applications and Protocols", vol 1 (2-3), 2003,pp.1293 –1303

[4] Dr. A. A. Gurjar, Professor, Department Of Electronics & Telecommunication, Sipna's C.O.E.T, Amravat and A. A. Dande, Second Year (M.E.), Computer Engineering, Sipna's C.O.E.T, Amravat "

Black Hole Attack in Manet's: A Review Study" International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, March 2013,pp. 12-14.

[5] D.Djen, L. Khelladi, and A.N. Badache, "A survey of of Security issues in Mobile Ad Hoc Network," Communication Surveys & Tutorials , IEEE,vol. 7 no. 4, ,pp. 2-28,2005.

[6] D.Boneh,C.Gentry,B.Lynn,H.Shachem,"Aggregate and Verifiably Encrypted Signature from Bilineer Maps ",Advances in Cryptology-EUROCRYPT'03,LNCS 2656,Berlin,Spinger-Veralg,2003,pp.416-432.

[7] Dr.Parminder Singh,Damanpreet Kaur," Approach to Improve the Performance of WSN during Wormhole Attack using Promiscuous Mode", volume 73,international journal of computer application, july 2013,pp 26-29.

[8] Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, April 1999, pp. 46-55.

[9] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, Apr, 2002, pp. 22-26.

[10] Hesiri Itserasinghe and Huirong Fu,"Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks", International Journal of Software Engineering and Its Applications,Vol. 2, No. 3, July, 2008,pp.39-54.

[11] H. Deng, W. Li, and D. P. Agrawal. "Routing Security in Adhoc Networks." In: IEEE Communications Magazine, Vol. 40, No. 10, Oct. 2002,pp. 70-75.

[12] Hongmei Deng, Itsi Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002,pp70-75.

[13] J. Cai, P. Yi, J. Chen, Z. Wang, N. Liu, An adaptive approach to detecting black and Grey hole attacks in ad hoc network, in: 4th IEEE International Conference on Advanced Information networking and Applications, IEEE Computer Society, 2010, pp.775–780.

[14] JiItsn CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An adaptive approach to detecting black and Grey hole attacks in Adhoc networks",24th IEEE International Conference on Advanced Information networking and application,2010,pp.775-891.1.

[15] K. S. Win, "Analysis of detecting wormhole attack in wireless networks," vol. 48, 2008, pp. 422–428.

[16] Latha Tamilselvan,V Sankaranarayanan,"Prevention Of Blackhole Attack in MANET",In proceeding of 3nd International Conference on Wireless Broadband and Ultra Wideband Communication, Aug 2007,pp.21-21

[17] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attackin wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), Apr. 2004, pp. 96-97.

[18] N. H. Mistry, D. C. Jinwala and M. A. Zaveri,"MOSAODV: Solution to Secure AODV against Black hole Attack", (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009.pp.42-45.

[19] O. Kachirski and R. Guha, "Effective intrusion detection using multiple sensors in wireless ad hoc networks", In Proceedings of the 36th Hawaii International Conference on System Sciences,2003, pp. 57-61.

[20] R.Agrawal, R. Tripathi, S. Tiwari, "Performance evaluation and comparison of aodv and dsr under adversarial environment", International Conference on Computational Intelligence and Communication Networks, IEEE Computer Society, 2011, pp.596–600.

[21] R.H.Jhaveri, S.J.Patel, D. Jinwala, "A novel approach for Greyhole and blackhole attacks in mobile ad hoc networks", Second International Conference on Advanced Computing and Communication Technologies, IEEE Computer Society, 2012, pp. 556–560.

[22] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3,Nov 2007, pp.338–346.

[23] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks",IEEE Transactions on Wireless Communications ,vol 1 (4) ,2002,pp. 660–670.

[24] X.P.Geo,W.Chen,"A Novel Grey hole Attack Detection Scheme for Mobile Adhoc Networks[C]",IFIP International Conference On Network and Parallel Computin Workshop,2007,pp. 209-214.

[25] Xiaoyan Hong, Kaixin Xu, and Mario Gerla, "Scalable Routing Protocols for Mobile Ad hoc Networks," IEEE Network,Vol.16(4),July/August2002,pp.11-21.

[26] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.

[27] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", TItsnty- Second Annual Joint Conference of the IEEE Computer and Communications Societies, Vol. 2, IEEE Computer Society, 2003, pp. 1293–1303.

[28] Y. Law, P. J. Havinga, "how to secure sensor network", International Conference on Sensor Networks and Information Processing, IEEE Computer Society, 2010, pp. 89–95.

[29] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc.4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.