Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Evaluation of Gray Hole Attack in Mobile Ad-hoc Network and proposed Solution

Sandeep Kumar*
Dept of Comp. CDLU,
Sirsa, India

Mrs. Sangeeta
Dept of Comp. CDLU,
Sirsa, India

Pramod Kumar Soni
Raj Rishi College,
Alwar, India

The mobile ad-hoc networks are vulnerable to Denial of Service (DoS) attacks. MANET has features like self organizing, working as router as well as host having dynamic topology. In MANET, nodes have limited resources like bandwidth, battery power and storage capacity. Gray hole attack is a kind of denial of service (DoS) attack in mobile ad hoc networks. It is specialized type of black hole attack which changes its state from honest to malicious and vice versa. Gray hole attack is an event that degrades the overall network's performance by intentional malicious activity. In this paper, it is proposed the mechanism against gray hole attack and improves the network performance in terms of throughput, packet drop rate, packet delivery ratio and normalized routing overhead

Keywords— MANET, Network layer Attack, Gray Hole attack, AODV;

I. INTRODUCTION

Mobile ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. In other words to make that work, typically each node need to act as a router to relay packets to nodes out of direct communication range. Under these circumstances, routing is much more complex than is conventional networks. Many of the possible solution are determined by the characteristics of the media, the behaviour of nodes and the data flow. Since research in ad hoc networking has resulted in such a large amount of routing algorithms and protocols, it has become more and more difficult to decide, which algorithm are superior to others under wha t conditions (E. Cheng, 2001).For the successful deployment. This is an important problem, since a wrong choice may have a severe impact on the performance, and consequently on the acceptance of new technology. Also providing just any protocol is not feasible, due to the different requirements on hardware and lower network layers. Further it would not make sense. Since all devices in an area would need to agree on one method of they want to communicate. A mobile ad hoc network is a collection of digital terminals equipped with wireless transceivers that can communicate with one another without using any fixed networking infrastructure. Communication is maintained by the transmission of data packets over a common wireless channel. The absence of any fixed infrastructure. Communication is maintained by the transmission of data packets over a common wireless channel. The absence of any fixed infrastructure, such as an array of base stations, makes ad-hoc networks radically different from other wireless LANs. Whereas communication from terminal in an "infrastructure" network, such as cellular network, is always maintained with a fixed base station, a mobile terminal in an Adhoc network cans communication range. In other to transmit to a node that is located outside its radio range, data packets are relayed over a sequence of intermediate nodes using a store and forward "multihop transmission principle. All nodes in an ad hoc network are requires to relay packets on behalf of a multihop wireless network.

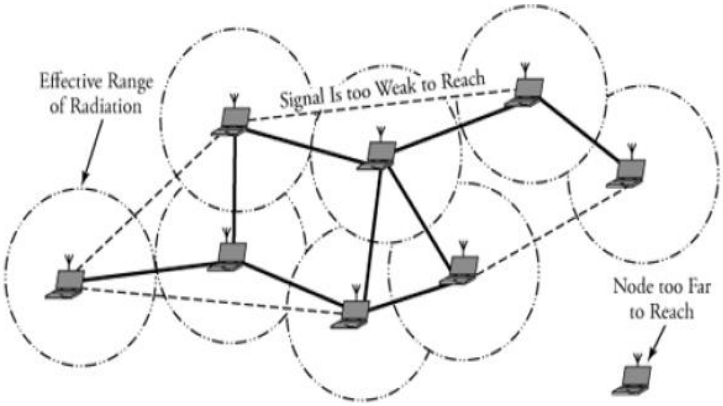

Figure 1 Typical MANET

II. ROUTING IN MANET

Routing in ad-hoc network involves determining a path from the source to the destination data can be communicated and the delivery of the packets to the destination nodes while nodes in the network are moving freely. Due to this node mobility, a path established by a source may not exist after a short interval of time. To cope with node mobility, nodes need to maintain routes in the network. Routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid and location-based categories depending upon how nodes can establish and maintain paths. Routing schemes can be classified into three categories namely, table driven (or proactive) routing protocols; On Demand (or Reactive) Routing protocols and hybrid (Location Based) routing protocols In Table-driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables for example DSDV, WRP. On Demand Routing (Reactive Protocols) these protocols take a lazy approach to routing. In contrast to table-driven routing protocols all upto-date routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. This section discusses a few on -demand routing protocols for example DSR, AODV. Ad hoc on-demand Distance Vector Routing (AODV) Ad hoc On-demand Distance Vector Routing (AODV) is an improvement on the DSDV algorithm discussed in earlier section. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. AODV requires each node to maintain a routing table containing one route entry for each destination that the node is communicating with. Each route entry keeps tracks of certain fields.

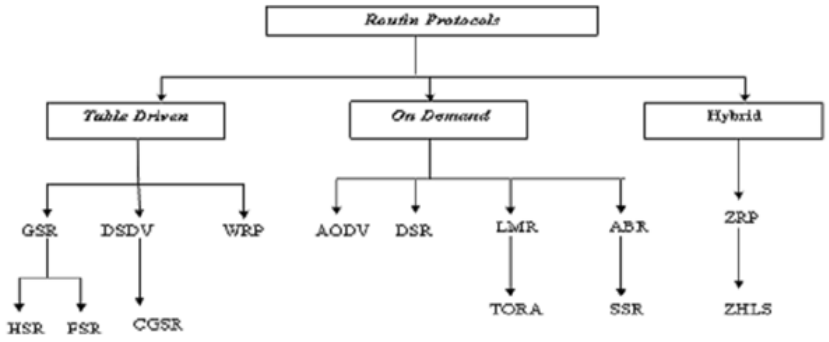

Figure 2 Routing Protocols in MANET

III. GRAY HOLE ATTACK IN MANET

Gray hole attack is kind of DoS attack where Gray hole node can attract all packets by pretending shortest route to the destination [12] [13]. It drops all traffic destined for that node when traffic is received by it. The effect of this attack completely degrades the performance of the network because the destination node never receives any information from the source. Gray hole attack is a specialization variation of black hole attack, where nodes switch their states from black hole to honest intermittently and vice versa. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to congestion. Figure 1 shows the gray hole attack. Detection is difficult because the node's nature is not stable, it can't predicted thatwhen node will be malicious and when it will turn to normal node.9th node selects gray hole even node 2 has valid and shortest path to destination.

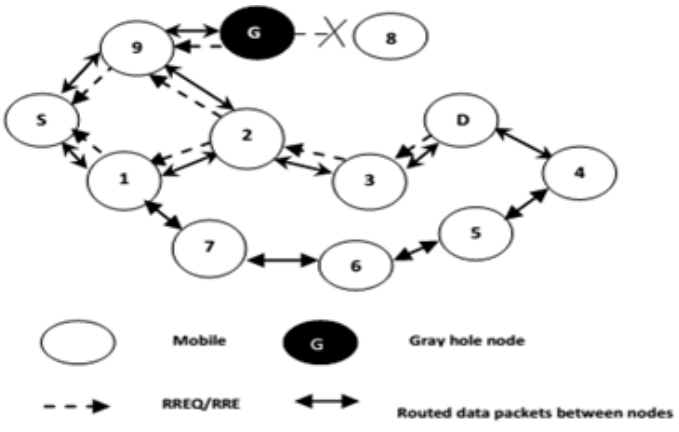

Figure : 3 Gray Hole Attack in MANET

IV. RELATED WORK

Neighborhood-based and Routing Recovery Scheme

Sun B et al. use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole/gray hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: Step 1-Collect neighbor set information. Step 2-Determine whether there exists a black hole/gray hole attack. In Response procedure, Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively and efficiently detects black hole/gray hole attack without introducing much routing control overhead to the network. Simulation data shows that the packet throughput can be improved by at least 15% and the false positive probability is usually less than 1.7%. The demerit of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets. This technique published in year 2003 and the simulation is done in NS-2 simulator.

Using watchdog/pathrater Scheme:

S. Marti, T. J. Giuli, K. Lai, and M. Baker (2000) proposed to trace malicious nodes by using watchdog/pathrater. In watchdog when a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet by promiscuously listening to the next node's transmissions. If the watchdog finds the next node does not forward the packet during a predefined threshold time, the watchdog will accuse the next node as a malicious node to the source node; The proposal has two shortcomings: 1) to monitor the behavior of nodes two or more hops away, one node has to trust the information from other nodes, which introduces the vulnerability that good nodes may be bypassed by malicious accusation; 2) The *watchdog* cannot differentiate the misbehavior from the ambiguous collisions, receiver collisions, controlled transmission power, collusion, false misbehavior and partial dropping. In *pathrater* algorithm each node uses the *watchdog's* monitored results to rate its one-hop neighbors. Further the nodes exchange their ratings, so that the *pathrater* can rate the paths and choose a path with highest rating for routing. Shortcoming of this algorithm is that the idea of exchanging ratings genuinely opens door for blackmail attack.

Counter- Threshold Based & Query- Based Scheme

D.M. Shila; T. Anjali (2008) offered a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The first stage of the algorithm is Counter- Threshold Based and uses the detection threshold and packet counter to discover the attacks. The second stage is Query- Based and uses acknowledgment from the intermediate nodes to confine the attacker. In the first stage, two types of packets, Control packet and Control ACK packet, are used to detect the attacker. Furthermore, they determine the proper value of detection threshold based on the routing Expected Transmission Count metric ETX to improve the performance under different network situation.

Aggregate signature algorithm

Gao Xiaopeng, Chen Wei (2007) proposed to use aggregate signature algorithm to trace packet dropping nodes. The proposal was consisted of three related algorithms: (1) the creating proof algorithm. (2) The checkup algorithm. (3) The diagnosis algorithm. The strengths of this suggestion are: (1) the reliability is satisfying, as proof on forwarded packets is used; (2) the application scope is wide, as bidirectional communication links are not necessary; (3) the security is satisfying, as it is hard for malicious nodes to flee detection; (4) the bandwidth overhead is low, as nodes do not need to check each other.

Centralized intrusion detection scheme based on Support Vector Machines

Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet S and Ekercio Glu (2007) presented a centralized intrusion detection scheme based on Support Vector Machines (SVMs) and sliding windows. This system can detect black hole attacks and selective forwarding attacks with high accuracy without depleting the nodes of their energy. They focus on adapting a simple classification based IDS to detect a specific spectrum of malicious DoS attacks, namely the Selective Forwarding Attack, that may be launched against a WSN. This IDS uses routing information local to the base station of the network and raises alarms based on the 2D feature vector (bandwidth, hop count). Classification of the data patterns is performed using a one-class SVM classifier. Support vector machines (SVMs) are a class of machine learning algorithms, due originally to Vapnik. While originally formulated for binary classification, they have since been extended to include regression, density estimation, and one-class classification. Over the last decade, SVMs have gained popularity due to their ability to tackle complex highly nonlinear problems in a consistent structured manner, while simultaneously avoiding problems of over fitting on simpler problem

Cross layer intrusion detection architecture based scheme

Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han (2010) proposed a novel cross layer intrusion detection architecture to discover the malicious nodes and different types of DoS attacks by exploiting the information available across different layers of protocol stack in order to improve the accuracy of detection. They used cooperative anomaly intrusion detection with data mining technique to enhance the proposed architecture. This architecture also detect sink hole attack at different layers of the protocol stack and detect various types of UDP flooding attack in an efficient way.

Channel appraised method

Vigilkumar V V, V. Mary Anita Rajam (2012) proposed a channel appraised method to detect colluding selective forwarding attack is considered. The detection is done in two phases. In the first phase, the channel estimation is integrated with traffic monitoring to achieve detection of selective forwarding attack, which can effectively identify selective forwarding misbehavior hidden in the normal loss events due to bad channel quality or medium access collisions. In the second phase, it integrate colluding node detection scheme with detection of individual selective forwarding attack.

TWOACK scheme

K. Balakrishnan, D. Jing and V. K. Varshney (2005) proposed a TWOACK scheme which can be implemented as an add-on to any source routing protocol. Instead of detecting particular misbehaving node, TWOACK scheme detects misbehaving link and then seeks to alleviate the problem of routing misbehavior by notifying the routing protocol to avoid them in future routes. It is done by sending back a TWOACK packet on successful reception of every data packet, which is assigned a fixed route of two hops in the direction opposite to that of data packets. Basic drawback of this scheme includes it cannot distinguish exactly which particular node is misbehaving node. Sometime well behaving nodes became part of misbehaving link and therefore can not be further used the network. Thus a lot of well behaved node may be avoided by network which results in losing of well behaved routes

Two-fold approach

Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, and Attique Ahmed (2008) proposed a two-fold approach for detection and isolation of nodes that drops data packets. First approach attempts to detect the misbehavior of nodes and will identify the malicious activity in network. It is done by sending an ACK packet by each intermediate node to its source node for confirming the successful reception of data packets. If the source node does not get ACK packet by intermediate nodes then source node send again its packet for destination after a specific time. If same activity was observed again then source node broadcast a packet to declare the malicious activity in the network. Other approach identifies exactly which intermediate node is doing malicious activity. It is done by monitoring the intermediate nodes of active route by the nodes near to active path which lies in their transmission range and by the nodes which are on the active route.

Adaptive approach based on a cross layer design

Jiwen Cai, Ping YI, Jialin Chen, Zhiyang Wang and Ning Liu (2010) proposed a method to detect black hole and gray hole in wireless ad-hoc network using an adaptive approach based on a cross layer design. In this paper, a path based method was used to overhear the next hop's action. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. The average detection rate is above 90% and the false positive rate is below 10%. After analyzing the merits and demerits of the above method, they proposed dynamic threshold and adaptive detection method to enhance the detection performance.

V. SIMULATION OF GRAY HOLE & RESULTS

To simulate the Gray hole attack we have used NS-2(2.28) simulator on CYGWIN environment. To implement Gray hole attack we need to define a new MANET Routing Protocol in NS-2. In this work we have used the nodes that exhibit Gray hole behavior in wireless ad-hoc network that use AODV protocol. Since the nodes behave as a Gray Hole they have to use a new routing protocol that can participate in the AODV messaging. All routing protocols in NS are installed in the directory of "ns-2.28". We start the work by duplicating AODV protocol in this directory and change the name of directory. Parameters for simulation are described in table 1

TABLE 1

Parameter	Value
Simulator	NS-2 (ver 2.28) on cygwin
Simulation time	500 seconds
Terrain size	1000 x 1000 sq.m.
Traffic type	CBR
CBR packet size	512 bytes/packet
Network protocol	TPC/IP (full duplex communication
MAC layer protocol	IEEE 802.11b
Routing Protocol	AODV
No. of nodes	20,30,40,50,60,70,80
Bandwidth	1 Mbps
Movement model (Mobility model)	Random waypoint
Maximal Speed	10 m/s
Interval Time To send	2 packets /seconds
Number of Connections	4,10,14,25

To test the implementation we used two simulations. In the first scenario we did not use any Gray Hole AODV Node. (The malicious node that exhibits the Gray Hole Attack will be called "Gray Hole Node"). In the second scenario we added a Gray Hole AODV Node to the simulation. Then we compared the results of the simulations using XGRAPH.
The goal of this work is to evaluate the performance of MANET under Black Hole attack. In this, the following section describes the qualitative metrices which are to be used to evaluate the performance of MANET.

Loss packet percentage (LPP)-loss packact Percentage is calculated by dividing the number of packets that never reached the destination through the number of packets originated by the CBR source

$$Loss \text{ Packet Percentage} = \frac{(sent \text{ Packets by CBR-Recieved Packets by CBR})}{Sent \text{ Packets by CBR}} * 100$$

Packet Delivery Ratio (PDR):- packet delivery Ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the CBR Source.

$$\text{Packet Delivery Ratio} = \frac{\text{Received Packets by CBR}}{Sent \text{ Packets By CBR}}$$

The PDR shows how successful a protocol performs delivery from source to destination. The higher for the value give the better results

EVALUATION OF RESULTS

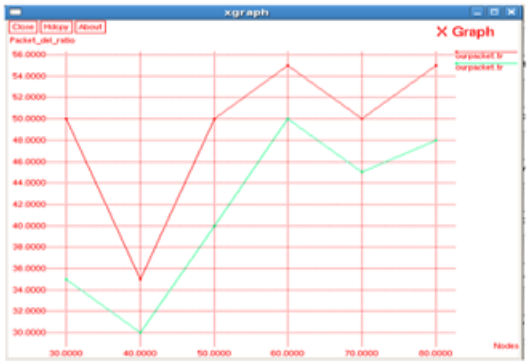

Figure 4. Comparison Graph of Packet Delivery Ratio

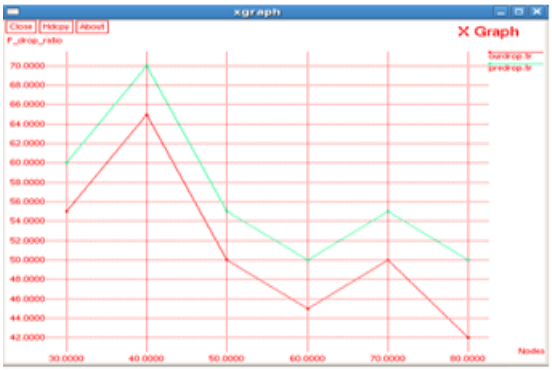

Figure 5: Comparison Graph of Packet Drop Ratio

Figure 6: Comparison Graph of Throughput

TABLE 2

Parameters	Under Gray Hole Attack	Without GrayHole Attack
Average Packet Delivery Ratio	60	70
Packet Drop Ratio	60 packets	50 packets
Throughput	12000 bytes/sec	13500 byte/sec
Average Network Life time	1700 ms	1800 ms

In this work has been carried out to study the effect of gray hole on the Network. This includes comparative analysis of the Network performance in the presence of a gray hole on the basis Average network life time, Average packet delivery ratio, Average packet drop Ratio and throughput. The overall performance of the network heavily decreases in the presence of a gray hole.

VI. PROPOSED WORK

Proposed algorithm is to detect gray hole node and eliminate the normal nodes with higher sequence number to enter in black list. The algorithm calculates the peak value and checks whether reply packet sequence number is less than or not. The parameters used to calculate the peak value are

(a) Routing table sequence number.
(b) Reply packet sequence number.
(c) Elapsed time of adhoc network which is analogous to current simulation time of simulator in simulation environment. Sequence number used in AODV protocol is 32 bit unsigned integer (2^{32}).This value is large enough so that maximum value will never reach. Continuous transmission upto 248 days at rate of 200packets/sec would be needed to exhaust this series. Adhoc networks are temporary. It would not operate for long duration exhausting the series suddenly.
(d) Total number of reply packets received by the intermediate/neighbor/replying node.
(e) Reply Forward Ratio (RFR) of replying node.

When the node gets detected, it would not send any alarm packet. Hence it is reduces routing overhead. Every node maintains a data structure in their local RAM which acts as a black list cum FALSE REPLY list of the nodes in the network. FALSE REPLY is the replies which are detected as a fake from malicious i.e. black/gray hole. Depending on the number of FALSE REPLY from the node it decides to be black listed or not. Using this approach, gray/malicious node is added to black list and eliminates normal nodes to enter in black list.

The conditions to add in black list are. e.g. if only one false reply is detected from normal node, It would not add to black list. If the number of false reply is detected from malicious node it adds to the list. Hence only one false reply does not add to list. It checks for the false replies from that node and then adds to black list.

Gray hole is a node switches from black to honest and vice versa. Whenever it switches to black, it will generate false reply which helps to detect it as a gray hole.Also it give every node on attempt/chance before adding to black list, hence resources for gray hole for packet forwarding can be utilized to some extent when they are normal state.

Algorithm for Gray Hole Attack

Step 1. Start (for each node which receives RREP).

Step 2. Check if a replying node has generated
False_Reply_Count greater than False_Reply_Threshold
if yes goto step 3,
else goto step 4

Step 3. Black list the node, don't accept any RREP packet (discard) from this node further.

Step 4. Check if routing table sequence number is less than reply packet sequence number.
if yes goto step 6
else goto step 5

Step 5. Skip detection engine and goto step10.

Step 6. Calculate
Difference between routing table sequence number and route reply sequence (Diff.).
RFR- Reply Forward Ratio
Peak = ([((Diff) × RFR) + No. of replies received by replying node + Current Simulation Time])/3

Step 7. Check if peak < route reply sequence number
If yes goto 8
else goto 10

Step 8. Increment the false reply count to corresponding replying node.

Step 9. Free the packet (RREP)

Step 10. Follow the remaining aodv recvreply() function

VII. CONCLUSION AND FUTURE WORK

Modified protocol, proposed approach uses effective way of providing security in AODV against gray hole attack. Proposed mechanism is to detect gray hole attack and eliminate the normal nodes with higher sequence number to enter in the black list. Effective decision making regarding black listing of nodes by keeping track on switching activity. Effective use of peak value and implementation of fresh approach of current elapsed time of adhoc network to make the proposed mechanism more efficient. It is not sending any alarm packets to other nodes when gray hole detected. Hence it is reducing extra routing overhead incurred by sending alarm packets.As a future scope of this work, the false reply threshold value which is static in this paper can be made dynamic based on elapsed time and predicted time for existence of network. Also to find cooperative environment to protect from gray hole attackers.

REFERENCES

[1] P. Agrawal, R.K Ghosh, S.K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", ICUIMC'08.

[2] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks " Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, " Mitigating Routing Misbehavior in Mobile Ad Hoc Networks." *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM)*, Boston, Massachusetts, United States, 2000, 255-265.

[4] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, issue 2, pp. 261-273, February 2006.

[5] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. "Prevention of cooperative black hole attack in wireless ad hoc networks." In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003

[6] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[7] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method" International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 1, January 2012)

[8] B. Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black-hole Attack in Mobile Ad Hoc Networks[C]; 5th European Personal Mobile Communications Conference, 2003, 490-495.

[9] A. Patcha; A. Mishra; Collaborative security architecture for black hole attack prevention in mobile ad hoc networks[C]; Radio and Wireless Conference, 2003, 75-78.

[10] D.M. Shila; T. Anjali; "Defending selective forwarding attacks in WMNs", IEEE International Conference on Electro/InformationTechnology, 2008, 96-101

[11] Gao Xiaopeng, Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", IFIP International Conference on Network and Parallel Computing Workshops 2007, pp. 209 -214.

[12] Xie Lei, Xu Yong-jun, Pan Yong and Zhu Yue-Fei. "A Polynomial-based Countermeasure to Selective Forwarding Attacks in Sensor Networks" - International Conference on Communications and Mobile Computing-2009, vol. 3, pp.455-459, 2009

[13] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari and Kumar Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", Fourth International Conference on Computer Sciences and Convergence Information Technology 2009, pp 824 – 828, Nov 2009.

[14] Tran Hoang Hai, Eui-Nam Huh "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge". Seventh IEEE International Symposium on Network Computing and Applications, pp.325-331, July 2008

[15] Sophia Kaplantzis, Alistair Shilton, Nallasamy Mani, Y. Ahmet S and Ekercio Glu "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines" Third IEEE international conference on Intelligent sensor, Sensor Networks and Information 2007, pp 335 – 340, Dec 2007sss

[16] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han. "A Novel Cross Layer Intrusion Detection System in MANET", 24th IEEE International Conference on Advanced Information Networking and Applications-2010, pp 647 – 654, April 2010.

