A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks

Ashok M. Kanthe
Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

Dina Simunic
Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

Ramjee Prasad
Director, Center for Tele-Infrastructure (CTIF), Alborg University, Alborg, Denmark

ABSTRACT
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 interms of throughput, packet drop rate, packet delivery ratio and normalized routing overhead.

General Terms
Routing Protocols, Performance, Security, Mobile Ad-hoc Networks, Intermediate nodes, Replying nodes, Source nodes.

Keywords
AODV protocol, Gray hole attack

1. INTRODUCTION
Mobile ad hoc networks are multi-hop temporary wireless network. It is dynamically formed amongst group of mobile hosts/nodes having wireless connectivity. It has different characteristics such as lack of centralized administration, distributed cooperation, changing topology without any existing infrastructure or backbone. Without fixed router or access point wireless nodes communicate with each other nodes acts as host as well as router. They communicate with each other within the radio range through wireless links. There are many research issues in MANET such as routing, power management, bandwidth management, radio interface and security issues. The applications of mobile ad hoc networks such as tactical networks, emergency services, commercial and civilian environments, home and enterprise networking, education, entertainment etc[1][2].

This paper presents the solution to gray hole attack and improves the performance of the network. The paper is organized like section 2 discusses about related work on routing protocol security, section 3 discusses about AODV protocol, section discusses 4 about gray hole attack, section 5 proposed mechanism, section 6 simulation and finally section 7 concludes the paper and future work.

2. RELATED WORK
J. Sen proposed a mechanism for detection of gray hole attack [3]. This mechanism requires four steps. In neighborhood data collection, Data Routing Information (DRI) table store data forwarding information, DRI table contains node number, from and through bits, ratio of request to send (RTS) to clear to send (CTS) and check bit. From stands the information on routing data packets from the node, through stands for information on the routing data packets through the node.DRI table identifies the suspicious node when from and through bits are zero. Local anomaly detection module contains Initiator Node (IN), Cooperative Node (CN) and Suspected Node (SN).The probe packet is not received to the CN, then IN will suspect about SN. In cooperative anomaly detection module, detection reliability is increased by reducing the probability of false detection of local anomaly detection.IN broadcasts the cooperative detection message to all the neighbors of the SN.IN constructs the probe check table. Node ID and probe status are the fields of probe check table. In global alarm raising module, it is sending alarm message to the all nodes in the network. This module is related to the gray hole attack detected by the cooperative anomaly detection algorithm. In this method, overhead of malicious node detection is high and speed of gray hole attack increases.

S. Kurosawa proposed an algorithm for detection scheme using dynamic learning method [4]. The training data is updated regular time interval. Destination sequence number is considered to detect the black hole attack. It is rise when the number of connections increases. The average of the difference between the Dst_seq_number in RREQ message and the number held in the list are calculated for each time slot. This method is not detecting the gray hole attack. As per the higher sequence number of the node entered in blocked list even the node is not malicious.

G. Xiaopeng proposed the detection scheme against gray hole attack [5]. It consists of three algorithms which are creating proof algorithm, the check up algorithm and the diagnosis algorithm. In creating proof algorithm, the source nodes are creating proof which is based on aggregate signature algorithm for received message. In check up algorithm, the source node suspects the malicious node. Reliability is good. Bidirectional links are not required. Security is satisfactory and bandwidth overhead is low. In diagnosis algorithm, the evidences are getting from the check up algorithm, it finds the malicious node. This mechanism is not detecting all malicious nodes.

S. Banerjee proposed a solution for detection and removal of chain of cooperative black hole and gray hole attack [6]. In this solution, all nodes monitor to each other. This mechanism examines against AODV protocol. Due to monitoring network it has high overhead and also consumes more energy for monitoring. Detection process for malicious node is slow.

DPRAODV solution checks to find Route Reply (RREP) packet sequence number which is higher than the threshold value [7]. It uses the concept of dynamic learning method, in which threshold value is dynamically updated through simulation [6]. If RREP sequence number is higher than the threshold value, then the node is suspected to be malicious and it will add in blocked list. It sends ALARM packet to the neighbors informing about malicious node. This protocol takes higher routing overhead due to ALARM packets. This modified protocol does not detect gray hole attack.

J. CAI proposal is based on cross layer design for detecting black and gray hole attack [8]. It is used two counters, collisionPktNum and noncolPktNum which are added in 802.11 protocols. Collision rate is calculated. The probability of node overhearing the next hop's forward action is calculated using overhear rate. The probability of collision calculated using Accumulated Collision Rate (ACR). The performance is evaluated interms of network throughput, false positive probability. It is evaluated in the grid simulation environment and random simulation environment.

Jhaveri R.H.[9] approach uses intermediate node dynamically calculating peak value, author used three parameters for calculation. RREP sequence number, routing table sequence number and number of replies received during time interval.

3. AODV Routing Protocol

AODV is reactive hop-by-hop routing protocol. It is based on Bellman-Ford distance algorithm. AODV find the route from source to destination only on demand [10] [11]. AODV protocol has different processes like path discovery, route table management, path maintenance and local connectivity management. In path discovery process source node communicate to the destination node through intermediate nodes. There is no routing information available in the table, path discovery starts by the broadcasting route request (RREQ) to all the intermediate nodes. RREQ contains source addresses, source sequence number, broadcast identity, destination address, destination sequence number and hop count. The concept of sequence number is taken from Destination-Sequenced Distance Vector Routing (DSDV) Protocol. The reverse path is setup automatically when RREQ packet is send reducing node (IN) produces the route reply (RREP) to the source node.

In forward path, it is the reverse of reverse path setup, RREP will setup route towards the destination node. RREP requires source address, destination address, destination sequence number, hop count and life time. In routing table management, each mobile node keeps the record of routing table entry of distinction. Routing table requires destination address, next hop, number of hops, sequence number of destination, active intermediate nodes and expiration time of route entry. In path maintenance, continuously hello messages are used to ensure that neighbors are available. If link is failed, route discovery process restarts and finds the route. In local connectivity management, nodes broadcast the hello messages to its neighbor's node for checking its availability.

4. GRAY HOLE ATTACK

Black hole attack is kind of DoS attack where black 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 that when 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.

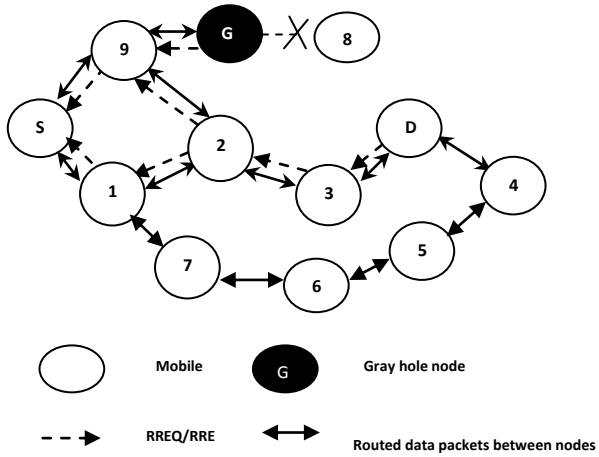


Figure 1. Gray hole attack

5. PROPOSED MECHANISM

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 [14] [15]. 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 200 packets/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.

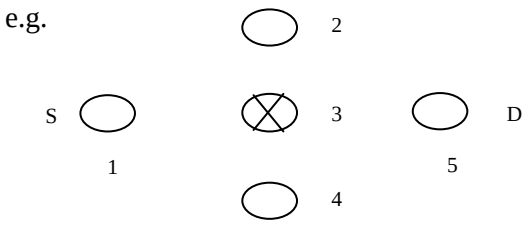
a) In this technique, detection of malicious nodes (m-node) is done during route discovery process. But the m_node is not black listed during first attempt of malicious activity. Whenever a malicious activity is detected by receiving node, it increases a false reply count for replying node in its local black list buffer (recv. node).

b) In this approach it makes 3 attempts of false reply to add a m_node in the black list. The attempts of false reply can be incremented as per scenario and elapsed time, node density.

c) Black list is local for each node. Each node maintains its own black list buffer. Information of the list is never broadcasted to any other nodes. The black list is private to each node individually.

d) Each and every node use detection and black listing locally. Hence any m_node will not broadcast false alarm packet pretending that particular node is malicious node (even it is normal) to other nodes in the network.

e) M_node is detected and black listed when receiving /source node detects malicious activity from replying nodes.

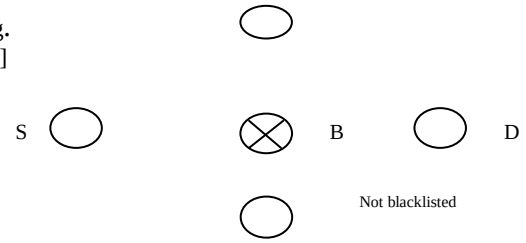


If S detects 3 as m_node it will not propagate alarm to 2 & 4. When 2 detects as a m_node it will not propagate alarm to its neighbors. Hence, scanning and detection is locally done and information is not broadcasted reducing routing overhead.

f) Gray holes are switching nodes from good to bad and vice versa. To detect them track has been kept on their switching activity.

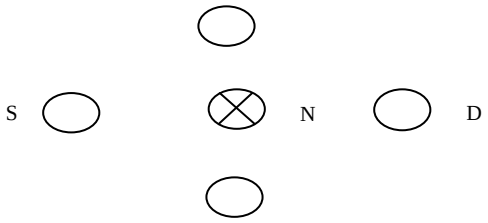
Hence it has used false reply concept.

e.g.
A]



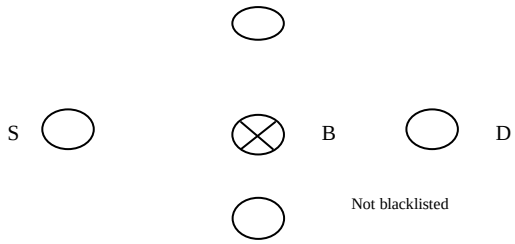
S receives first false reply from node B

B]



N is normal node which is not replying false reply packet.

C]



S receives second false reply from node B.
Hence at 3rd false reply from B, it is black listed by source node (S).

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,
no 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
no 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
No goto 10

Step 8. Add/Increment the false reply count to corresponding replying node.
Step 9. Free the packet (RREP)
Step 10. Follow the remaining aodv recvreply() function.

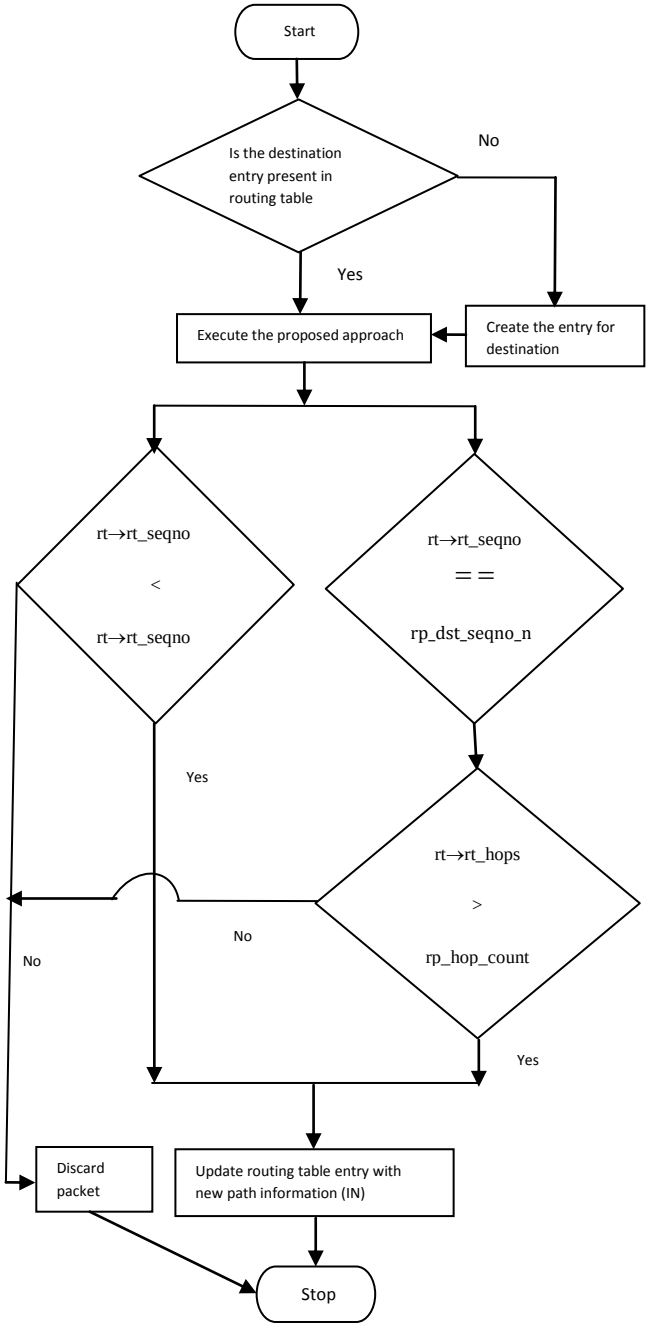


Figure 2.Flowchart for recvreply( ) function

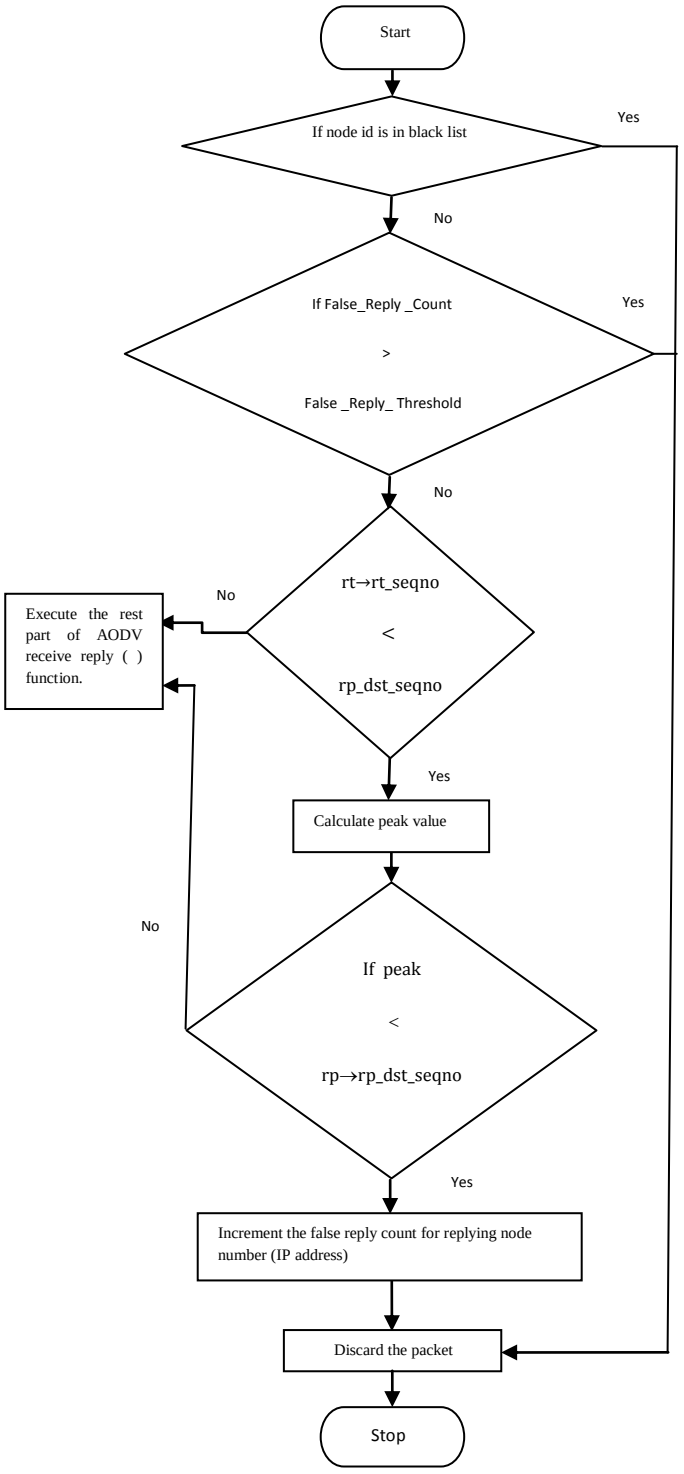


Figure 3. Execute the propose approach

Figure 2 shows the flowchart of recvreply function, figure 3 shows the execution the propose approach and figure 4 calculates the peak value.

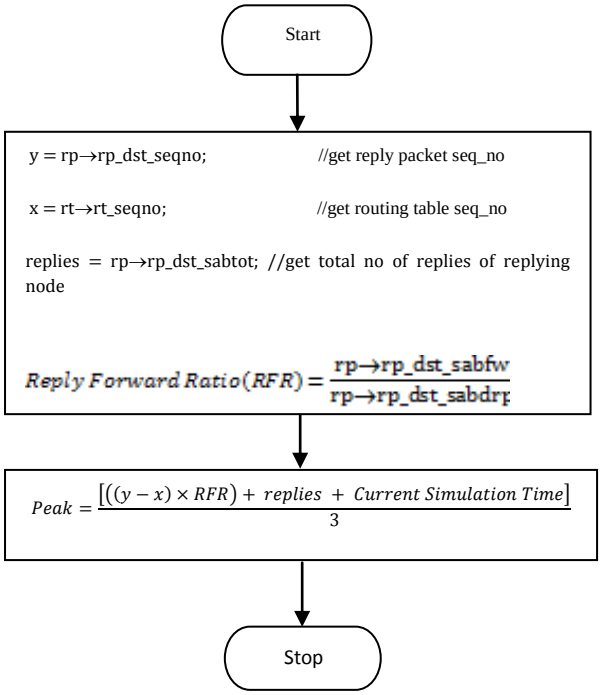


Figure 4. Calculate peak value

6. SIMULATIONS

We used simulation NS-2.35[16] having the simulation parameters shown in table I.

6.1 Simulation Environments

TABLE I. Simulation Parameters

Parameter	**Used in simulation**
Simulator	NS-2.35
DoS Attack	Gray hole attack
Channel Type	Channel/Wireless channel
Antenna Type	Antenna/OminiAntenna
Radio propagation model	Propagation/Two Ray Ground
Link Layer type	LL
interface queue type	Queue/ Drop Tail / PriQueue
Mac type	Mac/802_11
Protocols studied	AODV
Simulation time	100 sec.
Pause time	10 sec.
Simulation area	1500*1500
Trace format	New wireless format
Node movement model	Random waypoint
Traffic type	CBR(UDP)
CBR rate	50 Kbps
Data payload	512 Bytes/packet
Number of Malicious Nodes	1
Speed	50 m/sec.

6.2 Metrics

The metrics used to evaluate the performance of the mobile ad hoc networks are given.

Throughput: It is defined as the amount of data transferred over the period of time expressed in kilobits per second (kbps).

Packet Drop Rate: It is the ratio of the data lost at destinations to those generated by the CBR sources. The packets are dropped when it is not able to find the valid route to deliver the packets.

Packet Delivery Ratio: It is the ratio of data delivered to the destination to the data sent out by source.

Normalized Routing Overhead: It is the ratio of routing transmissions to the data transmissions in the simulations. The routing transmissions are RREQ,RREP, RERR etc.

6.3 Simulation Results

Performance of the AODV protocol is measured by varying the parameters in simulation like mobility, number of sources and number of mobile nodes.

All the results are dependent on current position of nodes i.e. simulation scenario and may vary on next simulation because the gray hole is flashing between good and bad. Time and duration for the gray-node to be white or black have been kept variable in TCL script using random number generator (random time) over the total simulation time (e.g. 100 sec).

When m_node is absent in network, on every simulation, results for normal aodv will be same.

But AODV attack and AODV under solution may vary,

Consider the below two scenarios

1. If random generator has assign long duration for white and short time for black.
2. Short time for white and long time for black.

Hence the value obtained from trace file using awk will give different values on every simulation. But on every simulation result gray hole attack will be worst and solution against gray hole attack will be neighboring to normal aodv (without attack).

Average end to end under attack reduces as the packets are dropping as they are not sent to destination. Average end to end delay under solution is greater due to extra calculation of peak value. Reply Forward Ratio is high for the normal AODV. It becomes low under malicious attack on the MANET. Number of replies received by replying node is high for normal AODV. It becomes low under malicious attack. Simulation studies shows that the performance of routing protocols in terms of throughput, packet dropping rate and end-to-end delay strongly depends on network conditions such as mobility, traffic and number of nodes. Figure 5,figure 6,figure 7 and figure 8 shows the graph for throughput, packet drop rate, packet delivery ratio and normalized routing overhead vs. mobility respectively. Figure 9,figure 10,figure 11 and figure 12 shows the graph for throughput, packet drop

rate, packet delivery ratio and normalized routing overhead vs. number of sources respectively.

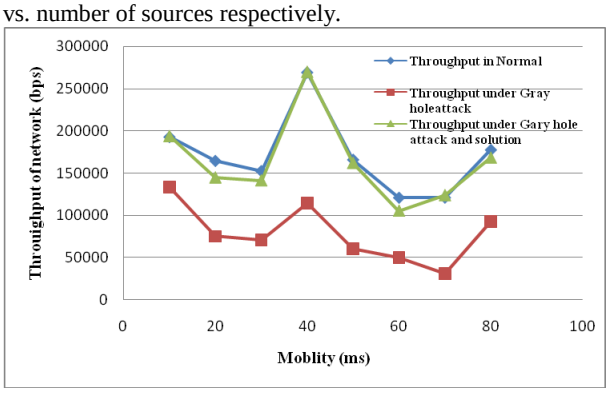


Figure 5. Throughput vs. mobility

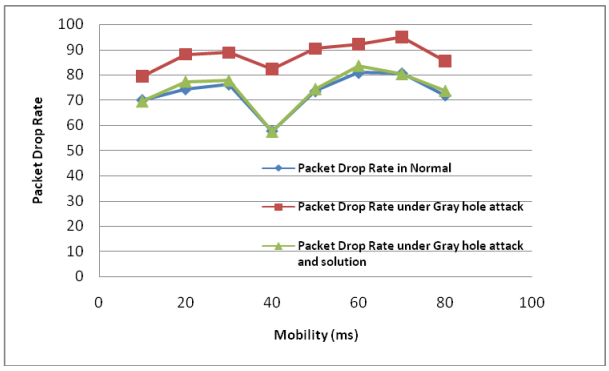


Figure 6. Packet drop rate vs. mobility

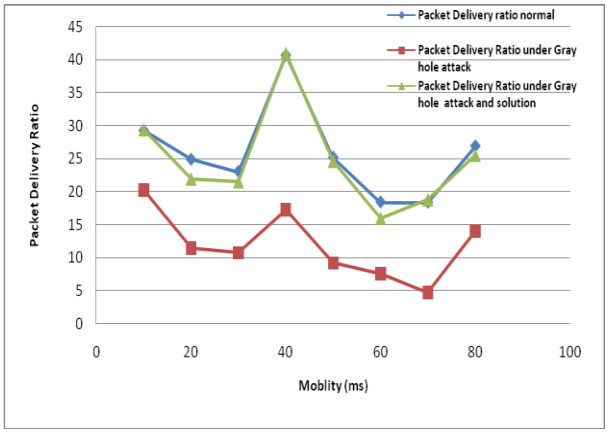


Figure 7. Packet delivery ratio vs. mobility

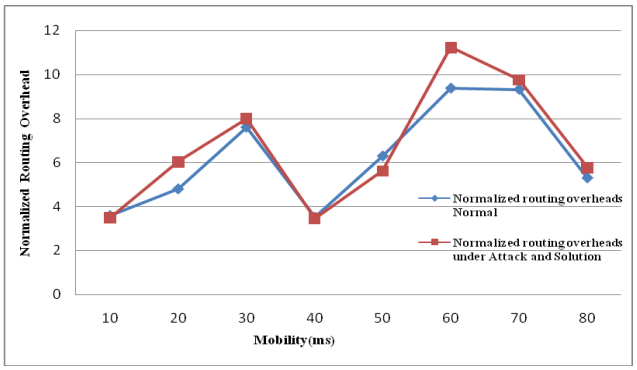


Figure 8. Normalized routing overhead vs. mobility

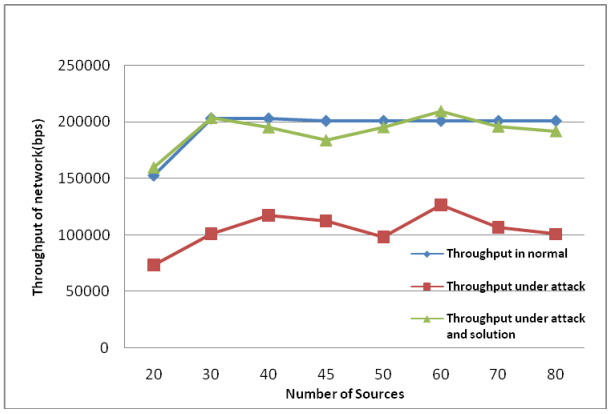


Figure 9. Throughput vs. number of sources

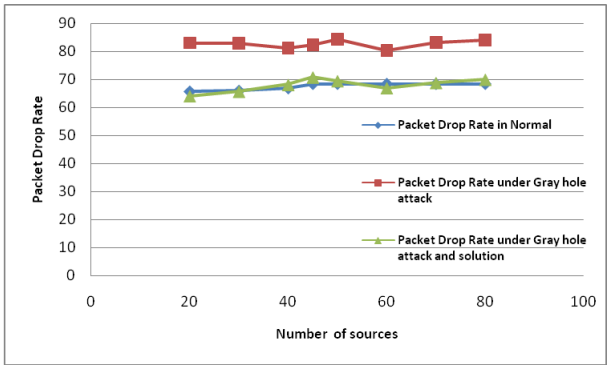


Figure 10. Packet drop rate vs. number of sources

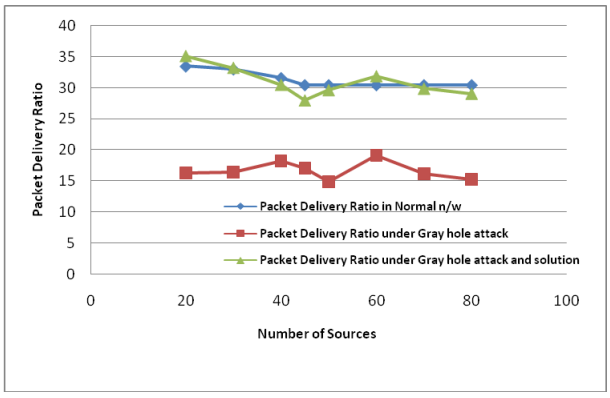


Figure 11. Packet delivery ratio vs. number of sources

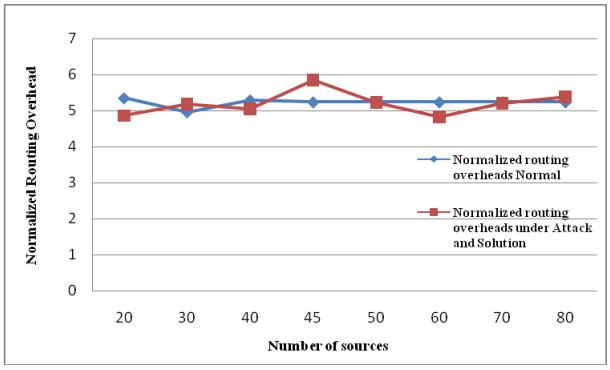


Figure 12. Normalized routing overhead vs. number of sources

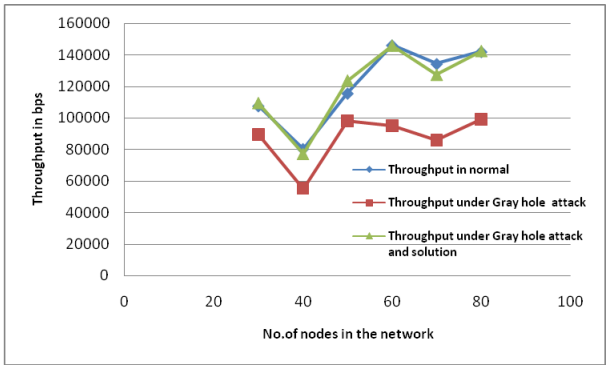


Fig.13 Throughput vs. number of nodes

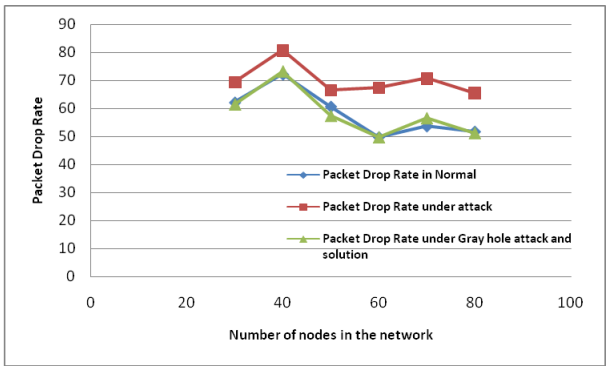


Figure 14. Packet drop rate vs. number of nodes

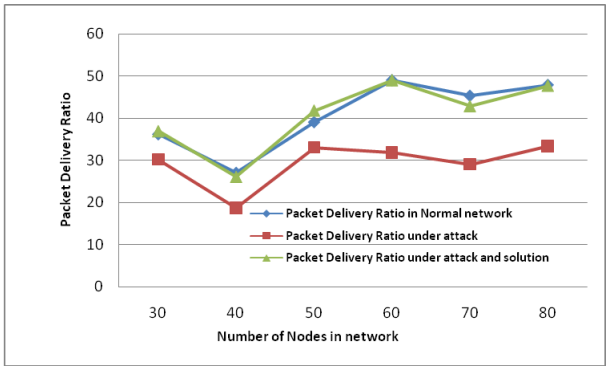


Figure 15. Packet delivery ratio vs. number of nodes

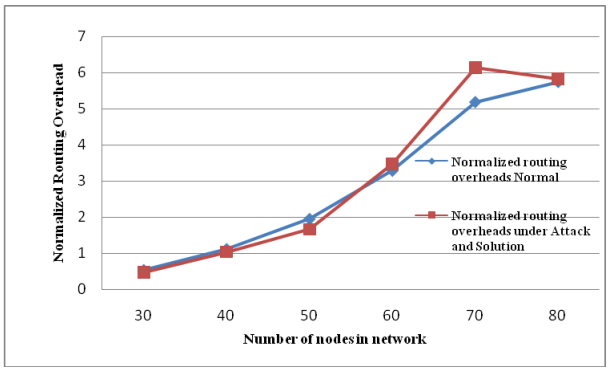


Figure 16.Normalized Routing overhead vs. number of nodes

Figure13,figure.14,figure.15 and figure.16 shows the graph for throughput, packet drop rate, packet delivery ratio and normalized routing overhead vs. number of nodes respectively.

7. CONCLUSION and FUTURE WORK

In 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.

ACKNOWLEDGMENTS

We would like to thanks Erasmus Mundus 'Mobility for Life' under the Erausmus Mundus External Cooperation Window Lot 11 for supporting the research work. Erausmus Mundus is a cooperation and mobility programme in the field of higher education, the promotion of the European Union as a centre of excellance in learning around the world and the promotion of intercultural understanding through cooperation with the third countries in the field of higher education.

REFERENCES

[1] C.K.Toh, "Ad hoc Mobile Wireless Networks :Protocols and Systems",Prentice Hall ,December 03,2001

[2] Jeroen Hoebeke,Ingrid Moerman,Bart Dhoedt,Piet Demeester, "An Overview of Mobile Ad Hoc Networks:Applications and Challenges"Journal of the communication networks,July 2004.

[3] Sen J.,Chandra M.,Harisha S.G.,Reddy H.,Balmuralidhar P., "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks",Information, Communications and Signal Processing ,2007,6th International IEEE Conference.

[4] Kurosawa S.,Nakayama H.,Kato N,Jamalipura A., and Nemoto Y. ,"Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning method,"International Journal of Network Security ,Vol.5,No.3,P.P338-346,Nov.2007.

[5] Gao Xiaopang, Chen Wei,"A novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks"Network and Parallel Computing Workshops,2007,NPC Workshops,2007,IFIP International IEEE Coference.

[6] Banerjee S,2008, "Detection/removal of cooperative black and gray hole attack in mobile ad hoc networks"In Proceedings of the World Congress on Engineering and Computer Science.

[7] Raj P N,Swades P B, "DPRAODV:A Dynamic Learning System Against Blackhole Attack in AODV based MANET,"International Journal of Computer Science 2:54-59,doi:abs/0909.2371.

[8] Jiwan CAI,Ping YI,Jialin CHEN,Zhiyang WANG,Ning LIU, "An Adaptive Approch to Detecting Black and Gray Hole Attacks in Ad Hoc Networks",Advanced Information Networking and Applications (AINA),2010th IEEE International Conference.

[9] Jhaveri R.H.,Patel S.J.,Jinwala D.C., "A Novel Approch for Gray Hole and Black Hole Attacks in Mobile Ad Hoc Networks",Advanced Computing & Communication Technologies (ACCT),2012 Second International Conference on 7-8 Jan 2012,IEEE, ISBN:978-1-4673-0471-9.

[10] C.Perkins, E.B.Royer,S.Das, "Ad hoc On Demand Distance Vector(AODV) Routing ,Internet Draft, " RFC 3561,IETF Network Working Group,July 2003.

[11] C.Perkins,E.B. Royer, S.Das, "Ad hoc On-Demand Distance Vector Routing," Proceeding of the 2nd IEEE Workshops on Mobile Computing System and Applications (WMCSA),pp.90-100,1999.

[12] Ashok M.Kanthe,Dina Simunic,Marijan Djurek, "Denial of Service (DoS) Attacks in Green Mobile Ad-hoc Networks",MIPRO 2012,IEEE Conference,Proceedings of the 35th International Convention,978-1-4673-2511-6,Opatija,Croatia.

[13] Elizabeth M.Royer,Santa Barbara,Chai-Keong Toh,"A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks",IEEE Personal Communication ,April 1999.

[14] P.W.Yau,S.Hu and C.J.Mitchell, "Malicious attacks on ad hoc network routing protocol," International Journal of Computer research ,15 no.1 (2007) 73-100.

[15] R.Perlman. Network Layer protocols with Benzantine robustness.Technical Report MIT-LCS-TR-429,Laboratory for computer science, Massachusetts Institute of Technology,October 1988.

[16] The network simulator-ns 2.35 http://www.isi.edu/nsnam/ns.