Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET

Shani Makwana
PG Scholar
Computer Engineering
RK University
Rajkot, Gujarat, India

Krunal Vaghela
Dy. Director
School of Computer Science
RK University
Rajkot, Gujarat, India

ABSTRACT

Mobile ad hoc network (MANET) is constructed from various number of nodes, that can be move anywhere and at any time, without any infrastructure. MANETs use wireless connections to connect various networks, without any fixed infrastructure or any centralized administration. Due to this nature of MANET, Ad hoc networks are open to different types of security attacks. The gray hole attack is the attack performed by the node called malicious node, which forwards and drops the selective packets only. Here, in this paper, we have proposed an algorithm which detects and eliminates the gray hole attack using Dynamic Credit Based Technique using AODV routing protocol. The gray hole node is detected based on credit value, which increases or decreases. The simulation results are compared with different situation and attempt to improve the performance of AODV protocol for the parameters like Packet Delivery Fraction, Throughput and End-to-End delay.

Keywords

MANET, security attacks, Gray Hole Attack, AODV Routing Protocol, NS-2.

1. INTRODUCTION

MANET is a self configuring, infrastructureless, connection less network of mobile nodes, in which each node act as router. The nodes are connected by wireless links without any centralised access point. In the network, all the devices are independent from each other. These devices are able to move and organize themselves randomly. Multi-hop paths are used for communication in MANET. The network topology is changes unreliably and dynamically in the wireless medium and all the nodes share the same network [2].

As nodes are open to move anywhere in MANET, the communication link breaks very frequently. In the MANET, according to applications, the number of nodes can be decided [2]. Military Applications, Emergency Operations, Wireless Mesh Networks, Wireless Sensor Networks are the applications of the MANET [2].

MANETs are exposed to different threats due to not having any infrastructure and dynamically network topology, which leads to different types of security attacks like Black hole Attack, Flooding Attack, Gray Hole Attack, Worm Hole Attack, Sinkhole Attack and many others [1].

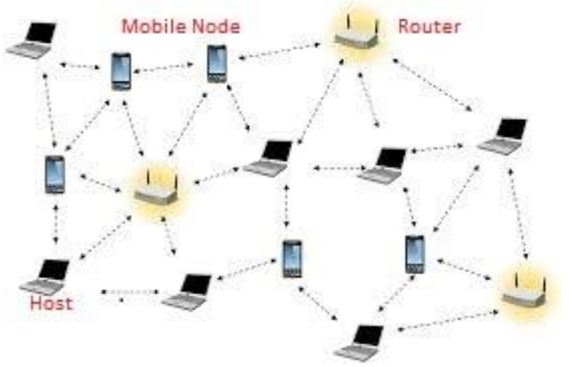

Figure1: Mobile Ad Hoc Network

2. AODV ROUTING PROTOCOL

The Ad-hoc On-demand Distance Vector routing protocol [3] is a Reactive Routing Protocol. AODV is a simple reactive routing algorithm and requires less memory with compare to proactive routing algorithm. In AODV, the route is created by the source node, whenever it needs. There are three control packets used in AODV, which are Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages. The use of RREQ message and RREP message is for route discovery and RERR is for maintenance of the routes [3].

In route discovery process, source sends RREQ packet in the network. Each node transmits the packet to its neighbor nodes until these packets reaches to the particular destination node or to earlier route towards destination, in the network. After that, source node waits for time until all the RREPs are received. Now the source node first check whether it has any entry in its table for that destination or not and then checks sequence numbers of the node. If the sequence number of the node is highest then, it selects that route for the transmission [13]. If there may present more than one RREP packets with the equal sequence number then, it selects the route with the minimum hop count to destination. If a link breaks, the maintenance process is required here. For that, neighbor nodes of that link broadcasts RERR message through the network to inform other nodes about the route failure. If this happen then, it is required to establish the route again to the destination [13].

3. GRAY HOLE ATTACK

Gray hole is a node that will act as a normal node that is actually an attacker node behaving like a black hole attack. So it is not easy to find the gray hole attack [12], since it behaves as a normal node. It is difficult to find out such kind of attack due to this type of behavior in the network. A routing table is maintained by every node that stores the information of the next node, which is a route towards the destination. The another name for gray hole attack is node misbehaving attack [12].

The gray hole attack perform its action in two different phases:

Phase 1:

With the purpose of interrupting packets on fake route, a malicious node performs the AODV protocol to give importance as only itself having a valid route to destination [4].

Phase 2:

The gray hole attack is difficult to find. In this the nodes drops the intermittent packets with a definite possibility. When the packets are not dropped, the gray hole attacker behaves like normal node then it switches to its malicious behaviour [4].

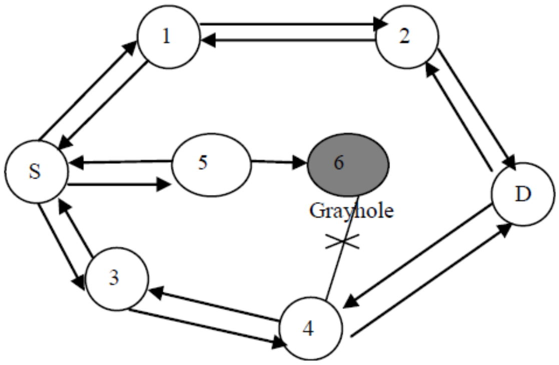

Figure 2: Gray Hole Attack

4. RELATED WORK

Onkar V. Chandure, V. T. Gaikwad [6] in this a distrustful node is found by examining its Data Routing Information table, when the security process is initialised by a node. Based on its DRI records, node transmits a RREQ message to only its nearest neighbour requesting for a route. The (Initiator Node) IN first selects a Cooperative Node (CN) in its region. The IN will receive many RREP messages from its adjacent nodes, from the Suspicious Node (SN), later which is really a gray hole.

Hizbullah Khattak, Nizamuddin [1] in the proposed solution, we have changed the system and it contains three different phases. In first part we have to make minor changes in AODV. Instead of using first path for transmission, it use second shortest path for data packets transmission. The packets are broadcasted in the whole network by the source node, which transmits the RREQ packet towards the destination. It may possible that malicious node can be presented in second shortest path also. To solve this problem, the unique message digest (MD) is calculated by applying hash function on the message [1]. Now source node transmits the MD with the data packets to the receiver. This MD is stored by the receiver node itself. A hash function is applied on the message to obtain a message digest again, when the receiver acquires all the data packets. After detecting the malicious node, Data Packets Received Error message is broadcasted by the receiver to the source node to again establish a route from source towards the destination.

Deepali A. Lokare, A.M Kanthe, Dina Simunic [7] in this proposed approach, the AODV protocol is a little modified and a new algorithm is known as Credit Based AODV (CBAODV). In this initially each and every node assigns a permanent value for its every adjacent node as the neighbor credit value. This credit value is increases by the protocol when it receives a route request packet (RREQ) and decreases when it receives the route reply (RREP) packet. When a node finds negative credit value for one of its neighbors, then it detected as the gray hole attacker.

D. C. Jinwala, S. J. Patel, R. H. Jhaveri [8] in proposed AODV protocol, node test the sequence number in routing table, when it receives a RREP packet. According to the sequence number is larger than the route reply or not, the RREP packet is accepted or rejected. The route discovery process is done here in the presence of a malicious node. The intermediate node enthusiastically calculates a highest value after particular time period. The calculated highest value, marked as Do_Not_Consider, when the node receives route reply packet with higher sequence number. When node sends RREP, the malicious node is marked in the routing table.

S. K. Das, P. Agrawal, R. K. Ghosh [9] there are some extra nodes-strong nodes, which help source and destination to find black and gray hole attacks. These strong nodes are supposed to be trustful. Also it has ability of tuning its antenna to short and large ranges. Each normal node is inside the range of one of these strong nodes. By using the strong nodes, source and destination begins to check, wether the data packets have been arrived to the destination or not. If any changes found in number of messages sent from source and received at destination, strong nodes ask the nodes in their areas about the monitoring results of one node’s behaviour. If the checking results show misbehaviour according to the votes, then the network runs a protocol which can detect black or gray hole attack. At last announces malicious node to the network by broadcasting messages.

Songwu Lu, Hao Yang, Xiaoqiao Meng, James Shu [10] SCAN uses two ideas to defend AODV in MANET: Local collaboration and Information cross-validation.

- In Local collaboration, nodes monitor each other and also maintain routing tables of each other. Each node uses a token that validates itself to the network. If one node is suspected to be malicious, other nodes invalidate its token and alert token revocation to all nodes in network and they insert that node in their token revocation list. So, the malicious node does not have any access to the network.
- In Information cross-validation, each node checks routing packets came from its neighbours. Each node knows every neighbour’s routing tables, which can cross-check the overheard transmissions of them.

S. Jain, M. Jain, H. Kandwal [11] In this approach, the gray hole attack detection and removal is done using source node, destination node and neighbor node. There are different detection as well as removal processes of Gray Hole Attack.

1. Black/Gray hole attack detection process by source node
2. Black/Gray hole attack removal process by source node

3. Black/Gray hole attack detection process by destination node
4. Black/Gray hole attack detection process by neighbor nodes
5. Black/Gray hole attack removal process by neighbor nodes

5. PROPOSED WORK

The proposed work contains the method to detect the gray hole nodes. All the nodes are initialized within the initial integer credit values. Then based on whether they are forwarding RREQ message successfully or not, credit value is increased or decreased. If a neighbour node receives a RREQ message from intermediate node then its credit value will be increased else the credit value will be decreased. i.e. if an intermediate node continuous send RREP message then credit value decreases and when credit value become zero, we observe DSN (destination sequence number), if DSN is too high with compare to SSN (source sequence number) that is-DSN is very large than SSN, then node identify as a gray hole node and simply not consider RREP and not select this route as a best Route. The node will not be ignored just based on one unsuccessful transmission, but its behaviour will be observed for some time.

By comparison of DSN number base on this hybrid scenario, we can conclude about gray hole attacker node. Credit value considered during initial routing process and it is stored in routing table. We compare DSN number through RREP message. So each node before forwarding RREQ message it stores receive DSN number hence, each intermediate node compares DSN number from receiving RREP message after credit values become zero.

In our work we do not compare DSN number every time because it consumes time and energy. We just increment and decrement credit value and only when credit values become zero at that time we will compare DSN number.

With the help of this proposed work we tried to improve Throughput, PDF and End-to-End Delay in MANET.

6. SIMULATION RESULTS

6.1 Performance Parameters

Throughput

The number of bytes received above transmitted per second is known as Throughput.

Packet Delivery Fraction (PDF)

The fraction of the count of delivered data packets at the destination node is called Packet Delivery Fraction.

End-to-End Delay

The time taken by a packet to be transmitted throughout the network from source towards the destination is called End-to-End Delay.

6.2 Simulation Parameters

The NS-2 (Version 2.35) simulator is installed in Ubuntu environment to simulate the results. We have analyzed the gray hole attack on AODV and proposed modifications in AODV here in this paper. The simulation results are compared with original AODV and proposed AODV results. For that the simulation parameters are presented in the table below.

Table 1. Simulation Parameters

Parameter	Value
Network Simulator	NS-2.35
Channel Type	Wireless Channel
Routing Protocol	AODV
MAC Protocol	802.11
Area	500 m x 500 m
Simulation Time	100 s
Pause Time	1.0 s
No. of Mobile Nodes	25, 50, 75, 100
No. of Malicious Nodes	1 to 5
Traffic	CBR (UDP)
Packet Size	512 Bytes/Packet
Maximum Speed	5.0 m/s
Mobility Model	Random Way Point

In the above simulation table, the different parameters like no. of nodes, pause time, simulation time, No. of malicious nodes are mentioned. The respective results of each scenario are shown from Figure 3 to 8.

6.3 Impact of Number of Nodes

Throughput

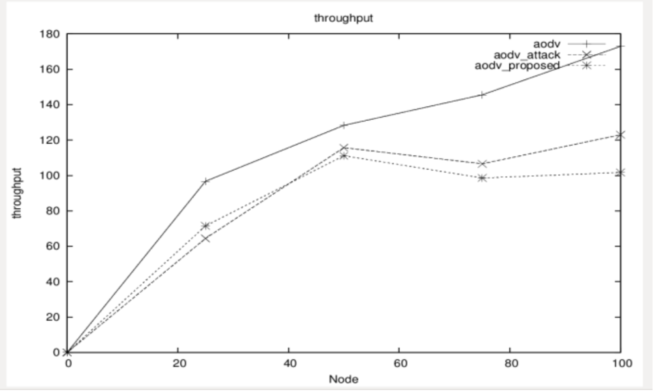

Figure 3. Throughput v/s No. of Nodes

Figure 3 shows the impact of increase of no. of nodes on throughput for protocol AODV, AODV with gray hole attack and proposed AODV. As the number of node increases, throughput is also increases. AODV protocol has highest throughput as it does not having any attacker disturbance in it. AODV protocol with gray hole attack has high throughput than proposed AODV. The performance of the proposed AODV is decreases here because the proposed AODV protocol finds the safe route to destination rather than AODV gray hole attack protocol finds, in which packets pass through more intermediate nodes, hence it takes more time to deliver the packet to the next safe node.

Packet Delivery Fraction

Figure 4 shows the impact of increase of no. of nodes on PDF. Here, the AODV protocol has a high PDF with compare to AODV with attack and proposed AODV because it takes safe route for data packet transmission and there is no disturbance of attacker node as it is a standard AODV protocol. AODV with gray hole attack having less PDF than AODV protocol because it shows its attacker behavior. It decreases the PDF, as it does not have any perfect method to prevent the data packet loss. Proposed AODV having lowest PDF than other two protocols, because it has to transmit more packets to find the safe and attack free route to the destination.

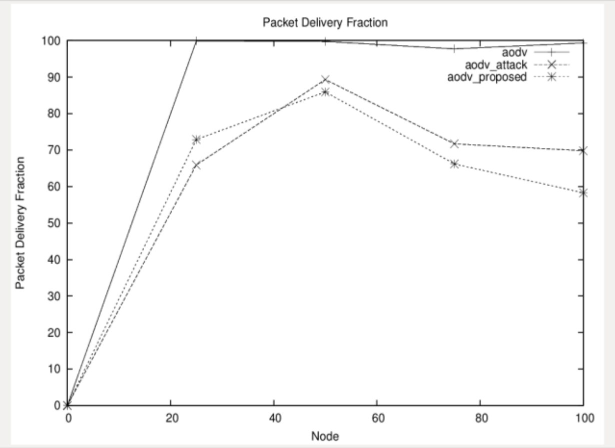

Figure 4. PDF v/s No. of Nodes

End-to-End Delay

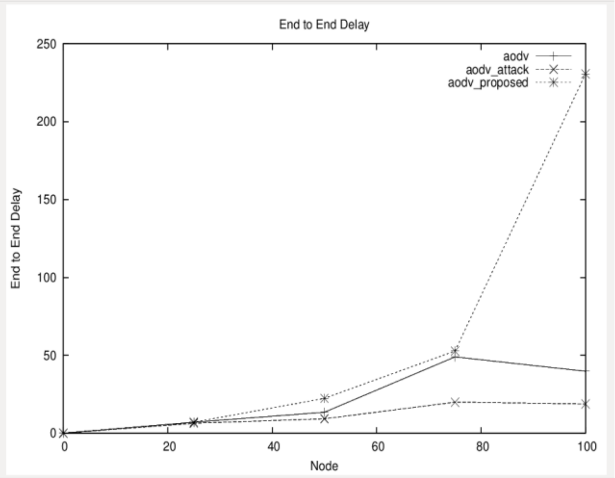

Figure 5. End-to-End Delay v/s No. of Nodes

Figure 5 shows the impact of increase of no. of nodes on end-to-end delay. Our proposed solution increases the delay with the increase of count of nodes. Here, proposed AODV protocol has a highest end-to-end delay with compare to AODV and gray hole attack. The reason behind this is that, it takes more time to search a safer and attacker free route from the overall network. The AODV with attacker node having lowest delay as the attacker nodes drops the packets. So, the packet could not reach to its destination on time.

6.4 Impact of Number of Nodes

Throughput

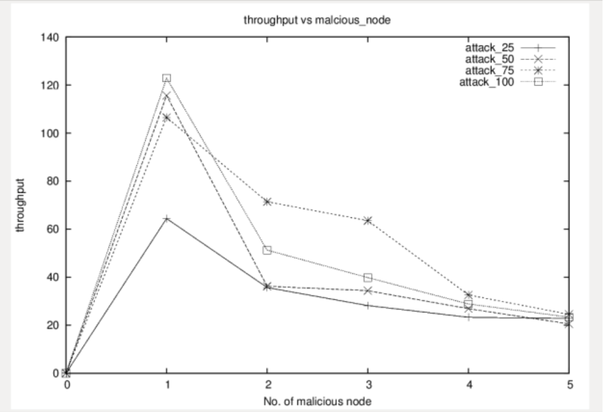

Figure 6. Throughput v/s No. of Malicious Nodes (AODV attack)

Figure 6 shows the impact of increase of no. of malicious nodes on throughput on AODV protocol with attack. The observation is that on the increases in count of malicious nodes, the throughput is decreases as the number of node increases in the network. The reason behind this is the malicious behavior of the attacker node, as packet cannot find next node to the destination which is attacker free.

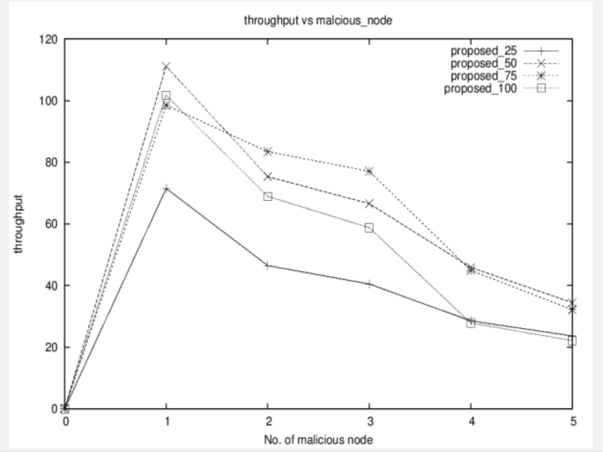

Figure 7. Throughput v/s No. of Malicious Nodes (proposed AODV)

Figure 7 shows the impact of increase of no. of malicious nodes on throughput on proposed AODV. The throughput for the different numbers of nodes is decreases, as we increase the number of nodes in the network because the no. of malicious nodes increases. This effect remains same for all the parameters on proposed AODV.

Packet Delivery Fraction

Figure 8 shows the impact of increase of no. of malicious nodes on PDF on AODV protocol with attack. As the number of malicious nodes increases, the PDF performance of the network is decreases. The reason behind this is malicious nodes drops almost packets because packets will not get safe and attacker free route in the network.

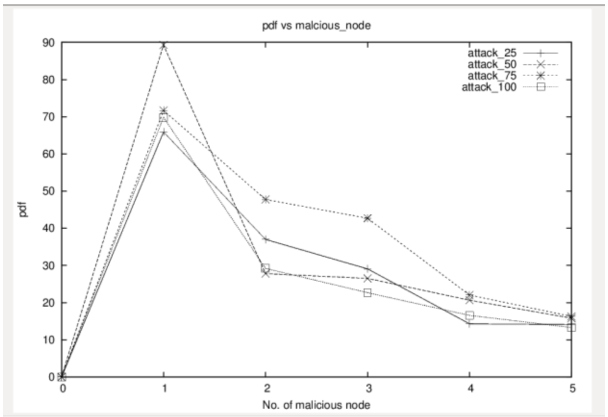

Figure 8. PDF v/s No. of Malicious Nodes (AODV attack)

Figure 9 shows the impact of increase of no. of malicious nodes on PDF on proposed AODV. The performance of the PDF is decreases less with the increase in count of malicious nodes compare to AODV having gray hole attack. The reason behind this is proposed AODV drops less packets than AODV gray hole attack.

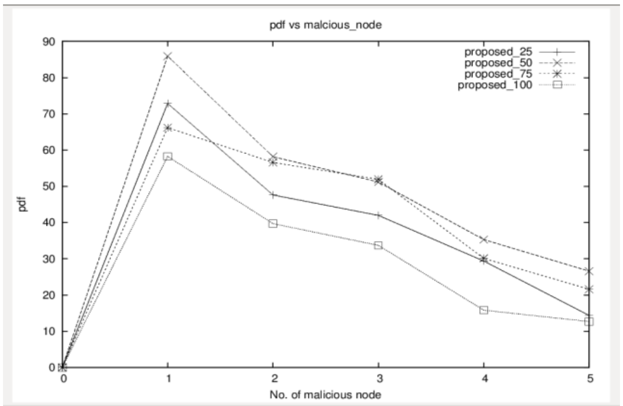

Figure 9. PDF v/s No. of Malicious Nodes (proposed AODV)

End-to-End Delay

Figure 10 shows the impact of increase of no. of malicious nodes on end-to-end delay on AODV protocol with attack. The end-to-end delay is decreases with respect to increases number of malicious nodes. Because of the number of RREP send by malicious node increases which congests all the paths of the network.

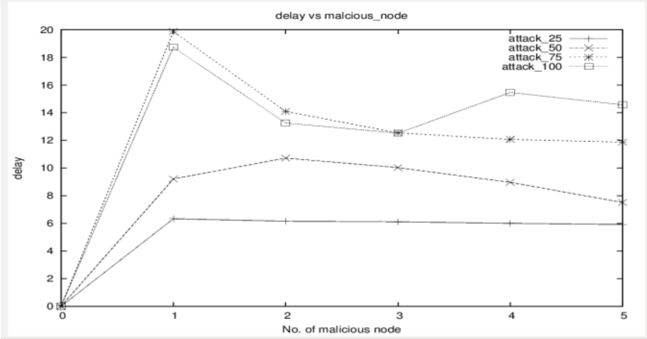

Figure 10. End-to-End Delay v/s No. of Malicious Nodes (AODV attack)

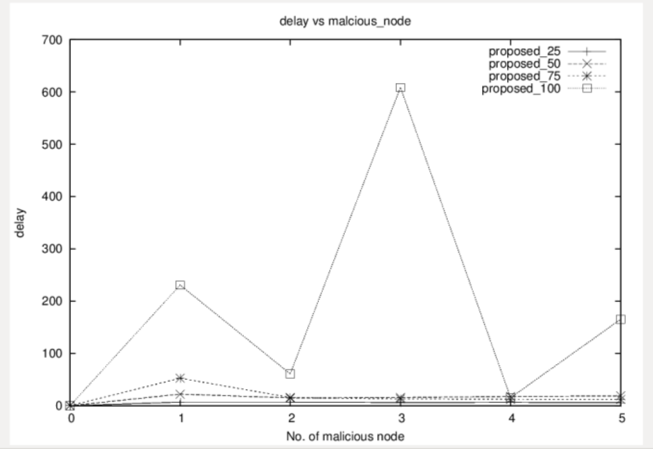

Figure 11. End-to-End Delay v/s No. of Malicious Nodes (proposed AODV)

Figure 11 express the impact of increase of no. of malicious nodes of end-to-end delay on proposed AODV protocol. The effect of decreasing the delay remains same for this protocol because of the nodes takes more time to find safe and attacker free route. The count of malicious nodes is increase the end-to-end delay is decreases as the no. of nodes presented in the network.

7. CONCLUSION AND FUTURE WORK

We have attempted to analyze and study different types of mobile ad hoc security attacks. There are some methods which are already implemented to solve this mitigation problem of attack. Because of lack of any centralized authentication or fixed infrastructure, the MANET security is the biggest challenge for the wireless network. The network suffers from various security attacks as the wireless link can be accessed by all and gray hole attack is one of them. In this paper, we have proposed a solution to detect and eliminate the gray hole attack using dynamic credit based technique using AODV routing protocol. The proposed algorithm is applicable for detection and elimination of the gray hole attack and the performance parameters like throughput, PDF and end-to-end delay are compared with the AODV protocol having gray hole attack in it. Here, we have analyzed that the performance of the parameters, which are improved with compare to AODV protocol having gray hole attack because of our strong proposed algorithm. In future this algorithm might be checked with other performance parameters on AODV protocol or on different routing protocol like DSR, TORA, OLSR, and GRP.

8. REFERENCES

[1] Hizbullah Khattak, Nizamuddin, “A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET”, Digital Information Management (ICDIM) Eighth International Conference, pp. 55-57, IEEE September 2013.

[2] M. Kumar, R. Mishra, “An Overview Of MANET: History, Challenges and Applications”, IJCSE, Vol. 3 No. 1, pp. 121-125, Feb-Mar 2012.

[3] Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi,“Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET”, IJCA Special Issue on “Network Security and Cryptography”, pp.11-17, 2011.

[4] Madhuri Gupta, Krishna Kumar Joshi, “An Innovative Approach to Detect the Gray Hole Attack in AODV based MANET”, International Journal of Computer

Applications(0975-8887), Volume 84- No.8, pp. 44-50, December 2013.

[5] Harsh Pratap Singh, Virendra Pal Singh, Rashmi Singh, “Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review”, International Journal of Computer Applications (0975 – 8887), Volume 64– No.3, pp. 16-22, February 2013.

[6] Onkar V. Chandure, V. T. Gaikwad, “Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol”, International Journal of Computer Applications(0975-8887), Volume 41- No.5, pp. 27-32, March 2012.

[7] Deepali A. Lokare, A.M Kanthe, Dina Simunic, “Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET”, International Journal of Computer Applications (0975-8887), Volume 88-No.15, pp. 13-22, February 2014.

[8] R. H. Jhaveri, S. J. Patel, D. C. Jinwala, “A novel approach for Grayhole and Blackhole attacks in Mobile Ad-hoc Networks”, Second International Conference on Advanced Computing & Communication Technologies, IEEE, pp. 556-560, 2012.

[9] P. Agrawal, R. K. Ghosh, S. K. Das, “Cooperative black and gray hole attacks in mobile ad hoc networks”, In Proceedings of the 2nd International C onference on Ubiquitous Information Management and Communication,pp.-310-314,January-2008.

[10] Yang, H., Shu, J., Meng, X., Lu, S., “SCAN: Self-organized network-layer security in mobile ad hoc networks”, IEEE journal, Vol. 24-No. 2, pp. 261-273, Feb-2006.

[11] S. Jain, M. Jain, H. Kandwal, “Advanced algorithm for detection and prevention of cooperative Black and Gray hole attacks in mobile ad hoc networks”, IJCA (0975-8887), Vol. 1-No. 7, pp. 37-42, 2010.

[12] Sukla Banerjee, "Detection/Removal of Coperative Black and Gray Hole Attack in Mobile Ad-hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008, October 22-24, 2008.

[13] C. Siva Ram Murthy, B. S. Manoj "Ad Hoc Wireless Networks: Architectures and Protocols".

[14] Garima Neekhra, Sharda Patel, Ashok Varma "A Literature Review on Detection of Gray Hole Attack in MANET AODV Routing Protocol" International Journal of Emerging Technologies and Engineering (IJETE), Volume 1 Issue 7, August 2014.

[15] Teerawat Issariyakul and Ekram Hossain, "Introduction to Network Simulator NS2 manual", 2009 Edition.

[16] Ashok M. Kanthe, Dina Simunic and Marijan Djurek, "Denial of Service (DoS) Attacks in Green Mobile Adhoc Networks", MIPRO, Opatija, Croatia, pp. 675-680, May 21-25, 2012.