IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 126-133
www.iosrjournals.org

Detecting multiple Blackhole and Grayhole attacks in MANETS by modifying AODV

Divya Khajuria
Department of computer science and engineering
Shri Mata Vaishno Devi University
Katra, India

Sudesh kumar
Department of computer science and engineering
Shri Mata Vaishno Devi University
Katra, India

Abstract: *Ad hoc networking refers to as network with no fixed Infrastructure. When the nodes are assumed to be capable of moving in the network, then networks are referred as MANETs (mobile ad hoc networks).Security is a paramount challenge in Ad hoc networks. Because of shared broadcast radio channels, insecure operating system, Limited resources, changing network membership, dynamic and arbitrary topology, no central authority, MANETs networks are sensitive and vulnerable to many security attacks. MANETs have critical application such as military applications and civilian application. In such applications, secure communication is of prime importance. Most of MANETs routing protocols works on trustworthy collaboration among participating nodes which leads to security threats. Lack of authentication and identification mechanism is another shortcoming in routing protocols due to which security issues arises in MANETs. There are many security attacks which occur on MANETs, Blackhole and Grayhole attacks being one of them. AODV protocol is effective and efficient in MANETs environment and is vulnerable to both Blackhole and Grayhole attack. A Blackhole attack is one in which malicious node falsely advertises itself as good path or stable path to destination during route discovery and malicious node starts dropping the packets instead of forwarding to destination.Grayhole attack is an extended version of the Blackhole attack where adversary behaves as a genuine node for certain time and turns into malicious node later on. In this paper, we proposed a modified version of AODV routing protocol that detect attacks before route discovery and during route discovery with high packet delivery ratio, low routing overhead and maintenance overhead.*

Keywords: *MANETs, Blackhole attack, Grayhole attack, fake RREQ.*

I. Introduction

MANETs suffer from various vulnerabilities than their wired counterparts encountered. An adversary may launch various attacks ranging from passive attacks to active interference. Passive attacks are one in which adversary intercepts the data exchanged in network without altering it such as eavesdropping. An active attack attempts to modify or destroy the data exchanged in network affecting the normal functioning of network. Packets modification and fabrication, message reply, denial of service attack (DoS) are some of examples of an active attack. Some of these vulnerabilities occur due to characteristics of MANETssuch as in-air-communication, limited resources such as Limited computation, lack of central administration, dynamic topology and changing network membership.

Vulnerabilities that are inherent to MANETs networks, reside in MANETs routing protocols. Most of routing protocols for MANETs assumes that all nodes will cooperate for communication and would not intentionally deviate from the protocols.

Ad hoc routing requires the participation of all the nodes in the network. Some attack by malicious nodes include sending false routing information, sending frequent routing updates to achieve denial of service and deviating traffic from legal route. Based upon routing information update mechanism, routing protocols for MANETs are divided into three categories: Proactive, Reactive and Hybrid. Proactive protocols (DSDV, GSR, HSR, and OLSR) are table-driven protocols in which the nodes maintain and update the routing tables periodically even when there is no communication. But in reactive protocols (AODV, DSR) or On-Demand Protocols, the routes are discovered on the demand of the source node. Proactive protocols have low latency exchange control messages and routing table information in order to keep up-to-date routes to any active node in the network. The reactive protocols have the low routing overhead at the expense of delay to discover the route when desired by the source. Due to periodically exchange of routing information, the proactive protocols are less prone to security attacks as compare to reactive protocols. The hybrid protocols (ZRP) have combined features of both reactive and proactive protocols.

In AODV [13], when a source has data to transmit to an unknown destination, it first checks its routing table and find whether route entry exist for destination in routing table. If yes then source node checks whether route is valid or not, if route is valid, it simply transmits the packets. If no, then source node initiates route discovery process to establish a route to destination. Source node generate RREQ message and broadcast to their

connected neighbours. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by-hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. Therefore at the end of route discovery process, packets can be delivered from source to destination.

In Blackhole attack, node sends fake routing information to advertise itself having an optimum path to destination and force other nodes to transmit data packets or discard traffic. The malicious node waits for the neighbours to initiate a RREQ packet. On receiving the RREQ packet, the malicious node immediately sends forged RREP packet with a modified higher destination sequence number. Source node believes that malicious node is having the fresh and shortest path to destination. Source node in turns ignores the RREP packet received from other nodes. Once the source node selects the forged route and starts to use it as delivery route for its data packets. Thus, all the packets are directed towards malicious node. The malicious node will deliberately drop all the received packets from source node. Blackhole attack can be of single or multiple types. Figure 1 depicts multiple Blackhole attack.

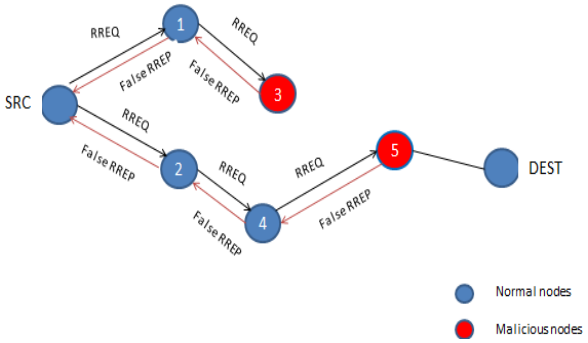


Figure1. Multiple Blackhole Attack

In Grayhole attack, node initially behaves normal then turns to malicious node after some time. A Grayhole may exhibit different malicious behaviour. It may drop packets either with certain probability or drop some packets corresponding to specific flow. It is an extension of blackhole attack where node drops the packet selectively. Such a Grayhole is known as selective forwarding. Another type of Grayhole node may behave maliciously for some time duration by dropping packets but may switch to normal behaviour later. A Grayhole may also exhibit a behaviour which is a combination of the above two, thereby making its detection even more difficult [11].

II. Related Work

Black Hole Attack Prevention System is given by [5] in Clustered MANET scheme to prevent Blackhole attack. A Friendship Table is created specifying the relationship of cluster head with its neighbour node. Source cluster head(S) broadcasts RREQ. When S receives RREP, S selects the shortest and next shortest path according to hop count. S checks Friendship table for one-hop neighbour nodes. If neighbour node is a friend then route data packet otherwise send false packets to the stranger and invoke the trust estimator. If trust value is out of tolerable range, stranger is assumed as a Blackhole node. This information is broadcasted to inform other nodes about malicious node. The disadvantage of this scheme is the increased routing overhead due to generation of False packets and also there is increased maintenance due to an additional Friendship table.

Moumita *et al.* [12] gives the proposed algorithm that works in two phases i) First phase detects those nodes, which may be malicious. Then the source node initiates the next phase. ii) In this phase neighbour of the malicious node initiates a cooperative detection mechanism to detect the actual Blackhole node. It requires each node to keep track of its neighbour by maintain two tables namely sequence table (SnT) and status table (ST); moreover, each node also maintains a neighbour list (N_List); When an intermediate node receives a RREP checks if the difference between the Dst_Seq present in the RREP message and the sequence no present in its table is greater than some predefined threshold value. if so then the intermediate node stops forwarding the message and mark the node as 'M' or malicious in the status table (ST); in the second step source node broadcasts and notifies all the neighbours of the suspicious node to cooperatively participate in the decision process; source node uses a Voter Table for gathering votes of neighbours for the suspicious node; during voting

process, Test Packet and Acknowledgement Packet are used to update the Voter Table. A Warning message is sent to notify other nodes in the network and update their Status Tables. The mechanism has drawback of adding significant overhead on each node for maintain numerous tables andTest Packet, Acknowledgement Packet and Warning message adds to routing overhead.

In Watchdog mechanism proposed by [6], every node keeps two extra tables pending packet table and node rating table. In pending packet table, each node keeps track of the packets which they sent. In node rating table, each node maintains rating of adjacent node.The last field of the node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node is considered as a misbehaving node, otherwise it is considered as a genuine node. Promiscuous node locally tells all the node of its wire-less range that particular node is misbehaving node. Discard RREP message coming from the misbehaving node. However, as the approach uses promiscuous mode, it consumes more energy, adds computational overhead to nodes and does not support directional antennas; adding to this, it adds overhead in terms of maintenance of two extra tables.

A solution to mitigate Blackhole and Grayhole attacks proposed by [7] in AODV based MANETS; it proposed a modified AODV viz. MR-AODV that isolates Blackhole and Grayhole nodes during route discovery phase by calculating PEAK value. PEAK value is obtained by adding three parameters- number of sent out RREQs, number of received RREPs and routing table sequence number to dynamically calculate PEAK value. Destination sequence number of received RREP is compared with this PEAK value to detect the existence of malicious nodes. The main advantage of this proposed solution is the reduced routing overhead. But this method cannot detect malicious nodes which set their destination sequence number less than PEAK value.

To reduce the probability of Blackhole attack, [2] proposed a method that wait and check the replies from all the neighboring nodes to find a safe route. The source node waits for the responses including the next hop details from other neighbouring nodes for a pre-determined time value. When time exceeds timeout value, it first checks in the CRRT (Collect Route Reply Table) table for repeated next-hop- node. If there exists any repeated next-hop, source node will assume that paths are correct and hence the chance of malicious nodes is less. The process of finding repeated next hop is an additional overhead.

III. Proposed Work

In this paper, a solution is proposed to detect the multiple Blackhole nodes and Grayhole nodes that can exist in the MANET. This method works in two steps: detection before route discovery and detection during route discovery.

During detection before route discovery phase, before actual route discovery process source node broadcast fake RREQ packet which includes destination address for node which does not exist in network [9]. The multiple Blackhole nodes will immediately send false RREP in respond to the fake RREQ packet as they do not care about whether the fake target addressed node exists or not in the network. The RREP packet is here modified by adding an extra field as Record Field using the reserved bits of RREP packet. This field will store the identity of the node who replies with the RREP packet to the source node. When any node in the network replies with RREP packet, its identity will be recorded into Record field. The routing table is also modified by adding one more field as malicious field. When source node receives RREPs in response to fake RREQ, it will mark those nodes as malicious nodes in the routing table under the malicious field. RREQ is also modified by creating backlist field using reserved bits. Then source node adds the list of malicious nodes to blacklist field in RREQ and broadcast to their neighbours to inform them about malicious nodes. Since RREQ itself is used to inform other nodes in network about malicious and no separate message is used, thus routing overhead is less.

During route discovery, nodes receiving RREQs firstly checks blacklist field in RREQ and mark those nodes as malicious nodes whose route entry exist in their routing table. The functionality of node receiving RREPs is enhanced [7]. Node receiving RREP will first checks whether the node that send RREP is marked as malicious node in its routing table. If yes then discard the RREP. If not then calculate PEAK value. The number of sentout RREQs, number of received RREPs and routing table Sequence number are used to dynamically calculate a PEAK value after every received RREPs; the PEAK value is calculated by adding these three parameters to the previous PEAK value. Destination sequence number of received RREP is compared with this PEAK value to detect existence of a malicious node. If destination sequence number of received RREP is greater than PEAK value, then corresponding node will be detected as malicious node and such malicious nodes are isolated by discarding the RREPs from these malicious nodes. Thus, this step detects and isolates multiple malicious nodes during route determination phase. If attacker generates destination sequence number less than or equal to PEAK value will not be detected but those nodes will be detected during first step.

IV. Algorithm Level design of Proposed Work

Notations: SN: Source Node IN: Intermediate Node DN: Destination Node

```
1. Start ( )
   {
2. SN broadcast the fake RREQ packet withnon-
   Existent target address;
3. If(one or more IN or Non-existent target nodes
   Reply back the fake RREP packet to SN) {
4. Trace the single or multiple black hole nodes from
   Record field of RREP packet and mark nodes as
   Malicious nodes in routing table.
5. Add the traced malicious nodes to the black list ;}
6. Initialize the normal AODV route discovery
   process and route maintenance process;
7. during route discovery,
8. Source node broadcast RREQ packet for route
   Discovery. RREQ is having black list field to
   inform other nodes know about the traced
   Malicious Nodes;
9. Nodes on receiving RREQ
    {
   Checks blacklist field;
   And mark those nodes as malicious nodes whose
   Route entry exists in their routing table.
   Isolate these nodes by discarding RREP from such
   Nodes   }
10. Node on receiving RREP message {
11. If sending node is marked as malicious node in
   routing table
12. Discard RREP;
13. If sending node is not marked as malicious node
   Then
   {
14. Calculate peak value
15. If RREP sequence no > peak
   {
16. Mark node as malicious node in the routing table
17. Discard RREP
    }
18. Else {
19. Update the routing table for the destination
   Sequence number
20. If (Receiving node is the source node)
21. {Discard RREP}
22.  Else
23.  {Forward RREP on the reverse path
    }}}}
```

RREQ: "BLACK LIST FIELD" containing list of malicious nodes is created using reserved bit.
RREP: "RECORD FIELD" containing identity of sending nodes is created again using reserved bits.
4 bytes of Peak value are allocated in memory. Two variables are required for calculation of peak value: no_of_sent RREQs and no_of_received RREPs (2 bytes each). Routing table is modified to include malicious_node field which is 2 bytes for each node entry.

This proposed solution enhances the security of AODV protocol with low routing overheads than other method [12] [5] in MANETs. No separate tables are used in the algorithm due to which maintenance overhead is reduced.

In addition to this no separate alarm message is used to inform others about malicious nodes instead RREQ is used which reduces routing overhead. The algorithm also ensures high detection rate. The detection of single or multiple black hole nodes have done early before the route discovery process in AODV. It makes this method more effective. During route discovery process, nodes detect malicious nodes whose destination sequence number are greater than Peak value and discard RREP from malicious node and don't send it to source

reducing routing overhead. But computation time for calculating PEAK value and sending fake request before actual request will add some delay.

V. Simulation Results And Analysis

In this section, first experimental setup is described followed by performance metrics, network scenario, simulation results and analysis.

A. Experimental Setup

NS-2 (Ver. 2.34) simulator installed in Red Hat operating system is used for performing experiments. BlackholeAODV and GrayholeAODV are implemented to add Blackhole and Grayhole behaviours respectively. Random waypoint model is used as the mobility model and Continuous Bit Rate (CBR) is used as traffic source; terrain area of 1100mx700m; packet size of 512 bytes; pause time of 2.0s; simulation time of 20s. The detailed Simulation parameters are presented in Table I.

Table I. Simulation Parameters

Parameters	Value
Terrain Area	1100mx700m
Simulation time	20s
MAC	802.11
Application Traffic	CBR
Maximum Bandwidth	2 Mbps
Routing protocol	AODV
Pause time	2.0s
Data payload	512 Bytes/Packet
Number of Nodes	10 to 40
Maximum Speed	10m/s to 50m/s
Number of Sources	5
Number of Adversaries	5

B. Network Scenario

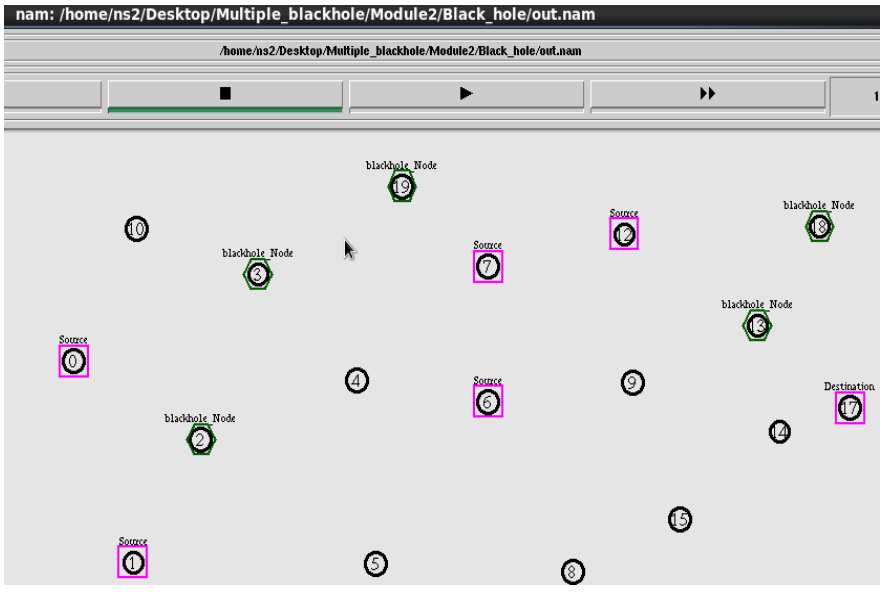


Fig. 2 Network Scenario

Network scenario created for evaluating AODV under Blackhole attack is shown in fig. 2. In this scenario node 0, 1, 6, 7, and 12 enclosed in pink box are source nodes and node 17 is the destination, whereas node 2, 3, 13, 18, and 19 enclosed in green hexagonal box are Blackhole nodes. Similarly, a same network scenario is created with nodes 2, 3, 13, 18, and 19 as Grayhole nodes for evaluation of AODV under Grayhole attack.

C. Performance Metrics

The metrics used to evaluate the performance are given below.

1) Packet Delivery Ratio**:** The ratio between the total number of packets received by destination nodes and the total number of packets generated by the source nodes.

2) Throughput: The number of successful bits per unit of time forwarded by the network from a certain source address to a certain destination.

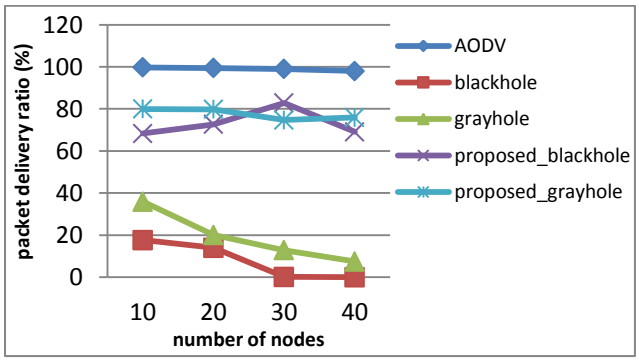
3) Normalized Routing Overhead: The ratio of total number of control packets to the total number of data packets.

D. Results

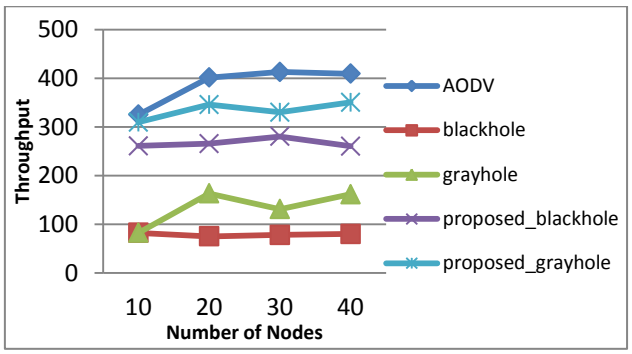
The performance of AODV is evaluated under multiple Blackhole and Grayhole attacks by varying network size and mobility.

1) Effect of Network Size: Number of nodes is varied from 10 to 40, keeping number of sources 5, number of malicious nodes 5 and maximum speed of 50 m/s. Fig. 3 shows the behaviour of AODV under attack with varying the network size. From the analysis of graph it is found that PDR of proposed algorithm under Blackhole attack is increased by 87% as compared to PDR of AODV under Blackhole attack. Similarly, PDR of modified AODV under Grayhole attack increases by 75%. Throughput is also increased in proposed work as compared to AODV under attacks. It is increased by 74% when proposed solution is run under Blackhole and 60% increment is there when solution is run under Grayhole attack. Routing Overhead for modified AODV is slightly increased in comparison to AODV because of generation of one extra control packet that is fake RREQ.

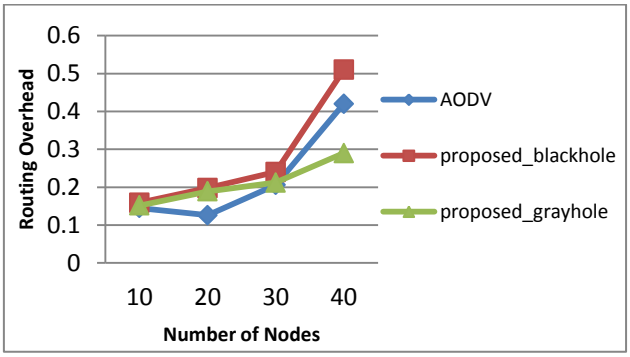
2) Effect of Mobility: The speed is varied from 10 m/s to 50 m/s with network size of 20, number of adversary 5 and no of sources 5. In AODV under Blackhole attacks, PDR and threshold decreases by 95% and 79% respectively. Whereas under Grayhole attack, PDR and throughput decreases 87% and 65% respectively. The effect of mobility shown in figure 4. PDR and throughput is increased by 97% and 74% respectively, when we apply proposed solution to AODV under Blackhole attacks. Modified AODV under Grayhole attack increases PDR and throughput by 85% and 52% respectively. There is slight increase in routing overhead under both attacks.



(a)

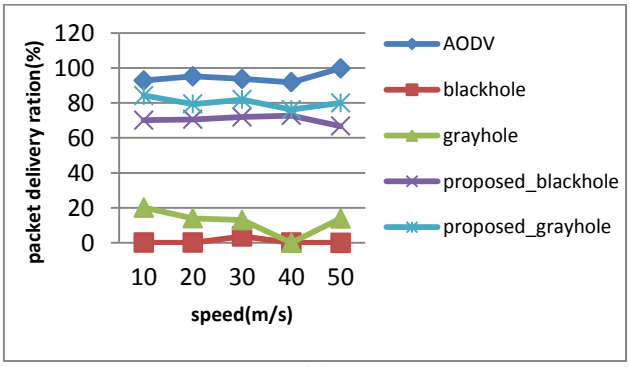


(b)

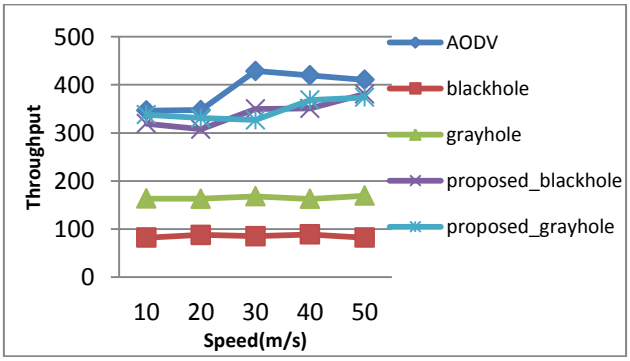


(c)

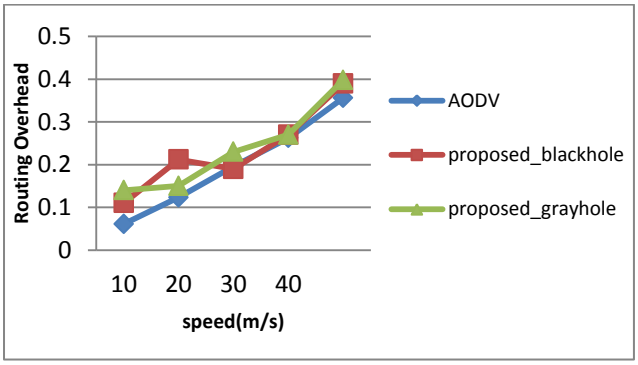
Fig. 3 Effect of Network Size



(a)



(b)



(c)

Fig. 4 Effect of Mobility

VI. Conclusion And Future Work

MANETs routing protocols are vulnerable to Blackhole and Grayhole attacks that affects their normal flow of data by sending forged routing information during route discovery and construction phase. This paper presents modification in AODV protocol for detecting multiple or single Blackhole and Grayhole nodes. Our proposed solution works in two steps: detection before route discovery and detection during route discovery. Our proposed solution results in less routing overheads as source node uses RREQ and RREP packets to inform other nodes about malicious nodes and does not use separate messages to inform other nodes. Our work also results in higher packet delivery ratio leading to higher detection rate. In future, we will improve our algorithm to reduce delay.

REFERENCES

[1] Hongmei Deng, Wei Li and Dharma P.Agarwal, "Routing Security in Wireless Ad hoc Network", IEEE Communications magazine, Vol.40, No. 10, 2002, pp70-75.

[2] LathaTamilselvan and V Sankarnarayan, "Prevention of Black Hole Attack in MANET", Journal of Networks, Vol. 3, No. 5,2008, pp 13-20.

[3] Mohammad Al- Shurman, Seong - Moo Yoon And Seungjin park, " Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd Annual Southeast regional conference, 2004, pp 96-97.

[4] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks" In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing services(CPS), January 2012, pp.556-560.

[5] IraNath and Dr.RituparnaChaki, "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2 Issue 8, August 2012, pp. 113-121. Moumita Deb, "A Cooperative Blackhole Node Detection mechanism for ADHOC Networks", In Proc. Of the World Congress on Engineering and Computer Science 2008, October 2008.

[6] Surana K.A., Rathi S.B. Thosar T.P. and SnehalMehatre,"Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms", World Research Journal of Computer Architecture, Vol. 1 Issue 1, 2012, pp. 19-23.

[7] Rutvij H. Jhaveri,"MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV based MANETS", Wireless sNetworks Security on Signal and Communication Technology Springer, New York, 2011. Rutvij H. Jhaveri,"MR-AODV: A Solution to Mitigate blackhole and Grayhole Attacks in AODV based MANETS", wireless Networks Security on signal and communication technology springer, New York, 2011.

[8] J.Sen, S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", Second International Conference on Intelligent System, Modeling and Simulation, Innovation lab, Tata consultancy services ltd., Kolkata, 25-27January 2011.

[9] KaliaNishu and MunjalKundan, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol", International Journal of Engineering and Technology, Volume-2, Issue-3, February 2013.

[10] Wang Huabin ,LuoZhongliang, " Research and Improvement of NS2- based AODV protocol in Adhoc Networks", Computer Era, No.5, 2011, pp. 12-14

[11] JayedipSen, M.GirishChander, Harihara S.G., Harish Reddy,P.Balamuralidhar, " A Mechanism for Detection of Garyhole attack in Mobile Adhoc networks", Proceedings of the 6th International Conference on Information, Communications and Signal Proceedings(ICICS), ISBN-1-4244-0983-7,December 2007.

[12] Moumita Deb, " A Cooperative Blackhole Node Detection Mechanism for ADHOC Networks", In Proc. Of the World Congress on Engineering and Computer Science 2008, October 2008.

[13] C.E.Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.