

Enhancing the Usage of MEDRI Table to Alleviate Blackhole and Grayhole Attacks in MANET

Manisha M. Jadhao¹, Rakesh Rajani²

¹ME student, Department of Computer Engineering, ACEM, Pune.

²Department of computer Engineering, ACEM, Pune

Abstract: Mobile Adhoc Network (MANET) is widely used where there is no pre-deployed infrastructure available. This is decentralized and dynamic topology network; hence it is vulnerable for different types of attacks. MANET often suffering from blackhole and grayhole attack, these are the one type of routing disturbing attacks and affected the network by major damaged and penalty. Hence to provide security to the network this paper focused a mechanism to alleviate blackhole and grayhole attack. The proposed method uses the Modified Extended Data Routing Information table (MEDRI) at each node and also used NACK (Negative Acknowledgement) algorithm which is used for detects and removes co-operative as well as non consecutive blackhole and grayhole attacks. This technique used under AODV protocol. The solution is capable to find out the multiple malicious nodes and maintain history of each node.

Keywords: AODV protocol, Blackhole attack, EDRI Table, Grayhole attack, Mobile Adhoc Network (MANET).

1. INTRODUCTION

A Mobile Adhoc Network (MANET) is decentralized network consisting of mobiles and wireless nodes where the nodes act as a router and carry data packets from one to other nodes. This network is categorized as dynamic topology because of nodes entered and leaves the network frequently. This network is very popular and used in learning, domestic purposes, business, and army services purposes. But the dynamic topology makes this network more vulnerable to different types of attacks and makes the network insecure to improve the security of network there is need to improve the security of Adhoc routing protocol, this paper focused on two types routing attacks that are blackhole and grayhole attack.

Blackhole attack is one kind of DOS (Denial of service) attack. A malicious node that is blackhole first replies to all route request (RREQ) that it has valid shortest route to reach to the destination node. This type of bogus route advertisement is made by the malicious node and it will try to attract all traffic of the network and redirected through itself. But it cannot forward the packet toward the destination but absorbed or stolen all the packets and hence this type of attack of malicious node is called as Blackhole attack.

Grayhole attack is somewhat similar to the blackhole attack, but the difference is that in grayhole attack the packet are partially dropped instead of total packet drop. Hence it is very difficult to detect the grayhole attack in the network because the malicious node uses the honest mask and forward the data through itself but during the transaction process it silently drop some packets, sometimes this happen due to overload, blockage or selfish nature of the node.

In the proposed work it is planned to alleviate the co-operative black hole and grayhole attack by introducing MEDRI (Modified Extended Data Routing Information) Table at each node in the network. The MEDRI table field's can easily find out the malicious nodes are blackhole or Gray hole and also maintain history of its malicious instances to avoid future malicious behavior of the nodes and make punishments that nodes who are always acting or notified in malicious instances. The proposed solution also planned to extend to achieve the non consecutive co-operative blackhole and grayhole attack.

The rest of the paper comprises: Section II literature survey, Section III Implementation Details, Section IV Mathematical Model and Section V wraps with Conclusion.

2. LITERATURE SURVEY

Many methods have been proposed to detect and prevent black hole and gray hole attacks by means of different approaches. Review of these methods is presented as below:

In 2013, Neha Kaushik and Ajay Dureja have proposed a solution to modify the AODV routing protocol in such a way that it can combat the cooperative Black Hole attack. The solution involves two additional changes in the AODV protocol. First change is the addition of two parameters in the routing table of each node in the network. These parameters are DATA_PCK_SENT and DATA_PCK_REC. Secondly, an additional routing table known as Routing Information Table (RIT) is to be maintained at source node. The purpose behind these two modifications is to increase the performance of AODV and eliminate the problem of Black Hole attack in MANET. The addition of RIT at source helps the source node

to check the reliability of the intermediate node and then forwarding data to this node.

Pros and Cons: The work shows an effective increase in throughput and PDR (packet delivery ratio) and decrease in average end-to-end delay with a slight increase in routing overhead [1].

In 2012, G. S. Bindra, A. Kapoor, A. Narang, A. Agrawal addressed a mechanism to detect and remove co-operative black hole and gray hole attacks by maintaining an EDRI (Extended Data Routing Information) Table at each node in addition to the routing table of the AODV protocol, the table is gradually updated as nodes interact with one another.

Pros and cons: The table maintains a history of its previous malicious instances to accommodate the gray behavior. The solution is capable to identify multiple black/grayhole nodes cooperating with each other in a MANET. But solution not works in detection of non consecutive co-operative blackhole and grayhole attack in MANET [2].

In 2011, Megha Arya and Yogendra kumar Jain focused on the detection of blackhole and grayhole attacks by using an intrusion detection system (IDS) to monitors the network or system activities for malicious activities or policy violation and produces reports to a Management Station. The Intrusion detection system (IDS) used for securing the AODV protocol which further named as IDSAODV Protocol.

Pros and cons: The simulation result shown that the throughput packet delivery improved rather than traditional Gray hole attack. But this work detect only gray hole attack and recover through IDS, means only routing misbehavior detection has done[3].

In 2010 Vishnu K. and Amos Paul addressed the proposed mechanism to detect and remove the attack on source node & intermediate node. Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted (unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (RIP) also. If any of the routes responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

Pros and cons: The solution worked to identify and remove any number of blackhole or grayhole nodes and discover secure path. But false positive effect of the solution not studied [4].

In 2010 Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU [5] proposed the a path-based method that is, a node does not watch every node in the neighbor, but only observes the next hop in current route path to detect black and grayhole attacks, After theoretically analyzing advantages and disadvantages of this method, they proposed an adaptive algorithm to enhance the detection performance. The simulation results reveal that attacks with gray magnitude above 60% would bring about magnificent damage to the network.

Pros and cons: The solution evaluate the positive and negative impacts brought by adaptive detection scheme, which provide a better false positive rate, but a less competitive detection rate also focused on the DSR protocol to test proposed algorithm and NS-2 as their simulation tool.

In 2008, Sukla Banerjee [6] focused on the problem of packet forwarding misbehavior and proposes a mechanism to detect and remove the black and grayhole attacks. In first phase the proposed method developed to handle the spiteful node in the network. And in the next phase of protocol is to implement the grayhole attack so as to recognize grayhole attack & find out its consequences on the ad-hoc network.

Pros and cons: The proposed technique is capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets. But the solution's performance against false positive feedback, throughput and packet drop ratio not studied.

In 2008 and in 2003 described a methodology to detect multiple black hole nodes that working collaboratively as a collection to begin cooperative black hole attacks. For the proposed solution the algorithm used the Data Routing Information (DRI) table and cross checking which using Further Request (FREQ) and Further Reply (FREP) to produce a slightly modified version of ADOV protocol.

Pros and cons: In both paper the DRI table used which recorded the data of routing but not sufficient for finding the gray behavior of nodes [7], [8].

From the observation of the various techniques it is found that the most researchers presented solutions and proved their correctness theoretically not proved effectiveness of their proposed solutions experimentally. Some techniques fail to detect grayhole attack as they are based on initial trust establishment.

3. IMPLEMENTATION DETAILS

A lot of work is carried out towards the implementation of detection and removal of blackhole and grayhole attacks by using DRI table and extended DRI table in MANET up to some area but still it remains demanding for a better solution

to eliminate attacks for secure packet transfer. Hence to progress in this area it is designed to develop MEDRI table and NACK algorithm to provide security to the network. The block diagram of proposed system is shown in Fig 1.

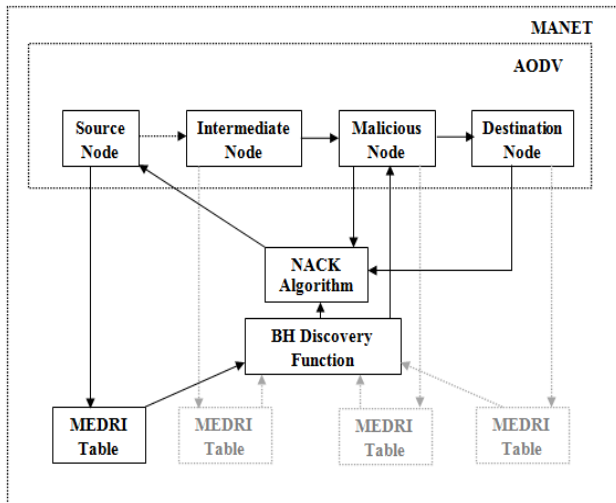


Fig. 1. Proposed Model

Step1: Implementation of AODV and MEDRI table

Step2: Implementation of NACK algorithm.

Step3: Implementation of BH discovery function to eliminate nonconsecutive co-operative blackhole and grayhole attack.

An ad-hoc routing protocol is a standard, that controls how nodes decide which way to route packets between computing devices in a mobile Adhoc network. On-demand protocols such as AODV (Ad-hoc On demand Distance Vector) establish routes between nodes only when they are required to route data packets.

The MEDRI table accommodates the gray behavior of nodes, it also keep records of the previous malicious instances of that node. MEDRI uses a counter which keep track on node and caught how many times the node behave as spitefully, if the node being caught for misbehaving frequently then not given a chance again.

With the existing RREQ and RREP packets, additionally used 'Refresh packet' and 'BHID packet'. A 'Refresh packet' sent by the source node through the different route with the help of NACK algorithm after sensing that node is misbehaving on that route. A 'BHID Packet' has the identity of the bad node. Algorithm helps to identify the bad nodes and disclosed their identity by broadcasting the 'BHID Packets'. This results in updating all their MEDRI entries for that bad node. Some more information about proposed algorithms is described in following sections.

A. AODV Protocol:

The function of AODV is to broadcast the route request and manage the path establishment in between source and destination.

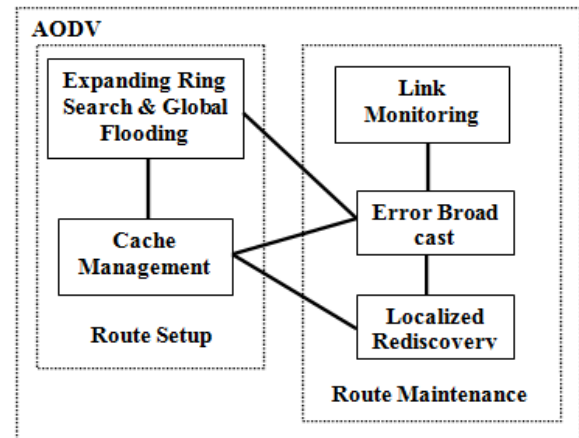


Fig. 2. Internal Architecture of AODV

The Internal Architecture of AODV as shown in Fig 2 comprises two main phases- Route Setup and Route Maintenance. Route discovery is the major mechanism in this phase. It is initiated if there is no cached route available to the destination. This mechanism consists of the following building blocks:

1. *Flooding building block*: The flooding building block takes responsibility to distribute the route request messages within the network. For range of flooding AODV uses the expanding ring search before the global flooding is initiated.

2. *Caching building block*: The caching building block helps to efficiently and promptly provide the route to the destination without referring to the destination every time. Caching block add route cache and route replay in the route setup also check Expiration Timer for route set up. Further, Route maintenance phase takes the responsibility of detecting broken links and repairing the corresponding routes.

1. *Error detection building block*: It is used to monitor the status of the link of a node with its immediate neighbors.

2. *Error handling building block*: It finds alternative routes to replace an invalid route after a broken link is detected. In Localized AODV, the upstream node detecting the broken link will initiate a localized flooding to find the route to the destination.

3. *Error notification building block*: It is used to notify the nodes in the network about invalid routes. The key parameter to this building block is the recipient of the error message. In a

localized recovery, the node detecting the broken link will attempt to find an alternative route in its own cache or do a localized flooding before asking the source to re-initiate the route discovery.

B. MEDRI (Modified Extended Data Routing Information) Table:

In proposed work it is planned to modify the existing EDRI table, though in the existing EDRI table fields such as ‘From’, ‘Through’, ‘CTR’, ‘BH’ and ‘Timer’ are present but still it is found inadequate for detecting gray hole attack, hence to overcome by such inadequacy it is planned to append three new columns such as ‘Source Packet size (SPS)’, ‘Destination Packet size (DPS)’ and ‘Result’ which checks the complete data packet reaches from source to destination or partial data reaches to destination. These three entries are very useful to catch the packet routing problem in MANET. Because of this MEDRI table network can easily find out the secure path from source to destination in MANET. An example of MEDRI table and its fields are as follows.

MEDRI TABLE.

Node_Id	From	Through	CTR	BH	Timer	SPS	DPS	Result
N2	0	1	1	0	0	12	12	Y
N3	1	1	0	0	0	12	12	Y
N5	0	0	2	0	0	12	8	N
N8	0	0	6	1	2 ⁹	12	0	N

- **FROM:** This entry shows the routed data packets from node that originated at the respective node id. Here 0 stands for false i.e. node has not routed data packets and 1 means node has routed data packets.
- **THROUGH:** Value 1 denotes that node id has successfully routed data packets that were sent by node else 0.
- **CTR:** CTR means counter that keeps a count of number of times the node behaved maliciously.
- **BH:** Entry 1 denotes that node id has been identified to be malicious in its latest interaction else it is 0.
- **TIMER:** This field has the duration count for which the node would be considered malicious.
- **SOURCE PACKET SIZE (SPS):** This field indicates the source packet size i.e. size of packet send by the source to destination.
- **DESTINATION PACKET SIZE (DPS):** This field indicates the destination packet size i.e. size of packet received by the destination from source.

- **RESULT:** This field is Boolean value which indicates the result. If the size of packets send from the source is equal to size of packets received at destination then result will be 0 or else it will be 1.

C. Current Status and network Layout.

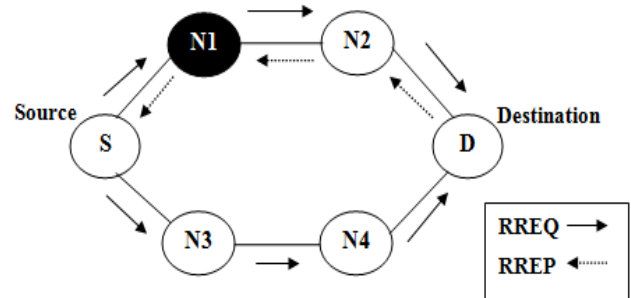


Fig. 3. Network Layout

Assume Current Status of Network is as follows.

1. Originally the network is free from any malicious nodes.
2. Source Node (S) wanted to send packets to Destination Node (D).
3. At the beginning all the MEDRI table entries for all other nodes are 0.
4. Node S broadcasts RREQ over the network.
5. It receives a RREP from destination D and the path (S-N1-N2-D) is established.
6. All the nodes update their MEDRI tables based on the RREQ and RREP packets sent and received.
7. At last the data packets were sent through the established path S-N1-N2-D and unfortunately Node N1 turns malicious and starts to drop packets. This affected on the data packets not reaches to the Node D.
8. After time out Node D sends out a negative acknowledgment to the source node S.

D. Algorithm for BH Discovery Function:

1. The Node S broadcast RREQ packet (Route request) for the destination Node D.
2. The IN (intermediate node) ie.N1 sends RREP with node id of NHN (next hop node) i.e. N2 and update its MEDRI entry for NHN.
3. Now the Node S checks its MEDRI entry for IN.

- If 'Through' entry for that node N1 is 1, means N1 is reliable node and it uses this path to transmit the data packets.
- Else it sends the FREQ (Further request packet) to NHN and checks it:
 - If IN has routed data through NHN.
 - The next hop for NHN in the route.
 - Has NHN routed data through its next hop?
- NHN replies with the FREP (Further Reply Packet) which has :
 - MEDRI entry for IN.
 - Next hop of NHN. (Node 4 here)
 - MEDRI entry for the next hop.
- If NHN is reliable for the source.
 - The source checks whether IN is a black hole or not. If the 'Through' column in IN's MEDRI table for NHN is 1 and the 'From' column in NHN's MEDRI table for IN is 0, IN is a blackhole.
 - If IN is found to be a blackhole, the source broadcasts this information. (Step 7 of the NACK algorithm)
 - Else the source updates its MEDRI table entries for IN. Now transmits Data packets
- If NHN is unreliable.
 - It checks whether IN is a black hole or not. If the 'Through' column in IN's MEDRI table for NHN is 1 and the 'From' column in NHN's MEDRI table for IN is 0, IN is a blackhole.

If IN is found to be a blackhole, the source broadcasts this information. (Step 7) Else make NHN as the new IN and next hop of NHN as NHN and goto step 3.

E. NACK Algorithm:

1. The Node D sends out a NACK (Negative Acknowledgement) across to the Node S through a different path here is D-N4-N3-S.
2. Now The Node S and Node D send a refresh packet along a concerned route i.e. S-N1-N2-D.
3. After the reception of a refresh packet, a node is supposed to do the following:
 - Set all it's 'From' and 'Through' MEDRI entries to 0.
 - Delete the route from its route table.
 - Pass the packet forward.

4. But the malicious node ignores this packet and does not forward it to the next node. (Because of this there is a need to send the packets from both directions so that all the nodes get it).
5. Now the Node S starts the Blackhole Discovery process using the BH Discovery function.
6. After detecting the malicious node's identity the Node S broadcasts it by sending out BHID packets.
7. Each node marks this node to be a blackhole by making entries in MEDRI BH field to 1 and increase the CTR value by 1.
8. Now each node starts a timer depending on the CTR value, which represents the time for the concerned node is to be considered malicious.

After timer expiration each node update MEDRI entry for BH field set as 0. And the node gets another chance for prove out his honesty.

F. Result:

The Solution shows expected result after complete execution. Following graphs shows the Network overhead and efficiency of the proposed.

The graph of Network overhead display that when we send Packets by 3 types like randomly, fixed interval and every time then NACK algorithm comes in picture every time packet sending then as NACK activity increases in network as well networks work increases it get busy for searching second path for sending data and network overhead increases continuously but if packet sending in fixed interval may send packet normally and NACK algorithm interference decreases. Hence Graph shows the solution perform best role with fixed interval time sending packet than the every time and random type.

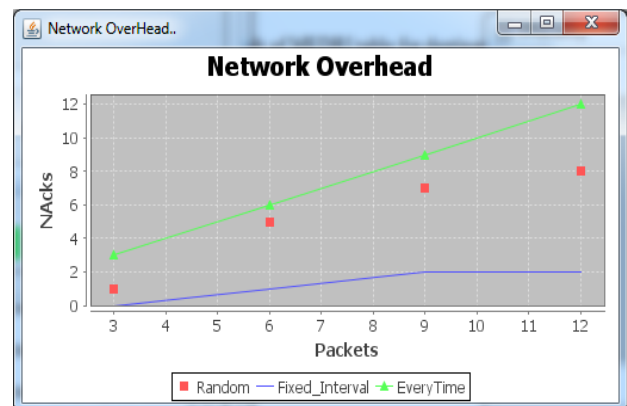
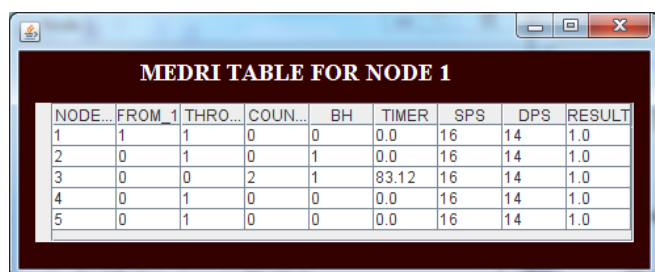


Fig. 4. Graph for Network Overhead

Let the source node broadcast the route request (RREQ) and establish the path from source to selected destination node by replying to RREQ with RREP and updating in the MEDRI table values with respective path. As the packet send toward the destination node BH discovery function start their working and detect the black hole is present in that path if present then broad cast that node as a blackhole after removal of that node record the time of node for acting as a black hole and update MEDRI values. After receiving the packet to the destination it sends ACK to the source if not received then destination send the NACK to the source. Following is the recorded MEDRI table after the successfully transitions of packet.

Table I: EDRI Table for Destination Node



NODE...	FROM	THRO...	COUN...	BH	TIMER	SPS	DPS	RESULT
1	1	1	0	0	0.0	16	14	1.0
2	0	1	0	1	0.0	16	14	1.0
3	0	0	2	1	83.12	16	14	1.0
4	0	1	0	0	0.0	16	14	1.0
5	0	1	0	0	0.0	16	14	1.0

The Efficiency of the proposed system is strong it provide solution in all type of data packets, if so many packets send randomly or every time or at fixed interval but defiantly the problem of grayhole and multiple black hole attack solved by the proposed system. The Efficiency of the system is shown following graph

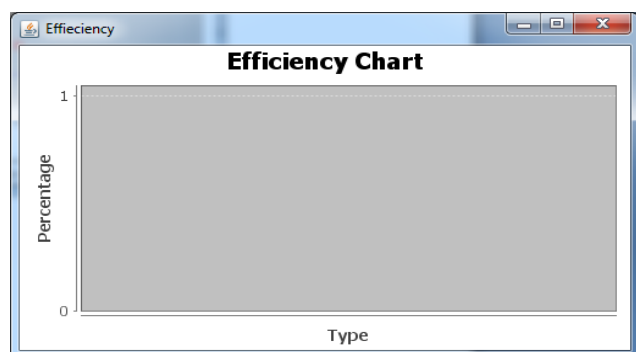


Fig. 4. Graph Efficiency Chart

4. CONCLUSION AND FUTURE WORK

Mobile Adhoc Network security is the today's biggest challenge. In the proposed work focus is on AODV protocol and on the co-operative blackhole and grayhole attacks in MANET and finding a feasible solution for detecting and removing them. In extension work towards detecting co-operative blackhole attack and grayhole attack as well as non consecutive co-operative blackhole and grayhole attack is carrying out. The MEDRI table also record and maintain the

history of the previous malicious nodes that is used for the future secure transformation of data from source to destination and to discover secure path from source to destination.

5. ACKNOWLEDGMENT

I would like to express my sincere thanks to my Guide Prof. Rakesh Rajani, Assistant professor Of Alard College of Engineering and Management, Pune for his consistence support and valuable suggestions. I am also thankful to all authors and researchers whose work has been a great motivation for leading me on right track.

REFERENCES

- [1] Neha Kaushik, Ajay Dureja, "Performance Evaluation of Modified AODV Against Blackhole Attack in MANET", *European Scientific Journal*, June 2013 edition vol.9, No. 18, pp.182-193.
- [2] Gundeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal "Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs" *IEEE International Conference on System Engineering and Technology* September 11-12, 2012, Bandung, Indonesia.
- [3] Megha Arya and Yogendra Kumar Jain "Gary hole attack and prevention in Mobile Adhoc Network" *IJCA* Vol.27, No.10. Aug 2011.
- [4] Vishnu K and Amos J Paul "Detection and removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks" *IJCA* Vol.1, No.22 Jan 2010.
- [5] J. CAI, Ping YI, Jialin CHEN, Z. WANG, N. LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", *Advanced Information Networking And Applications. (AINA) 2010 24th IEEE International Conference*, pp 775-780.
- [6] 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.
- [7] Hesiri Weerasinghe, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and valuation", *International Journal of Software Engineering and Its Applications*, Vol. 2, No. 3, July, 2008, pp: 39-54.
- [8] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". *In Proceedings of 2003 nternational Conference on Wireless Networks (ICWN'03)*, Las Vegas, Nevada, USA, pp. 570-575.
- [9] Rutvij H. Jhaveri , Sankita J. Patel, "DoS Attacks in Mobile Ad-hoc Networks: A Survey" 2012 *IEEE, Second International Conference on Advanced Computing & Communication Technologies*, pp. 535-540.
- [10] Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Sha hla Ghasemi "Methods of Detecting and Preventing Black Hole/Gray Hole attacks on AODV based MANET" *IJCA Special Issue on "Network Security and Cryptography"* NSC, 2011, pp. 11-17

- [11] Manisha Jadhao and Vani Hiremani, "Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET", *IEEE ICGCE-2013*, RMD college, Chennai, 1109/ICGCE.2013.6823448; Publisher: IEEE, pp 944-948
- [12] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao "A survey of black hole attacks in wireless mobile ad hoc networks" *Human-centric Computing and Information Sciences 2011, a SpringerOpen Journal 1:4*
- [13] B.Revathi, D.Geetha, "A Survey of Cooperative Black and Gray hole Attack in MANET" *International Journal of Computer Science and Management Research Vol 1 Issue 2 September 2012*.
- [14] Sarita Choudhary, Kriti Sachdeva. Discovering a Secure Path in MANET by Avoiding Black/Gray Holes. *International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-3, August 2012*.
- [15] Sweta Jain, Jyoti Singhai, Meenu Chawla, "A Review Paper on Cooperative Blackhole and Grayhole Attacks in MANETs". *International journal of Ad hoc, Sensor & Ubiquitous Computing Vol. 2, No. 3, 2011*.
- [16] Onkar V.Chandure, Prof V.T.Gaikwad " A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET" *IJCSIT*, Vol.2, No.6, Jul 2011.