Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Approach for Detection and Prevention of Various Types of Attacks in MANET

Ravinder Kaur
M.tech Department of Computer Science, Punjabi University, Patiala,
Punjab, India

Abstract— Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. In this paper detection and prevention mechanism for black hole attack and routing attack is implemented. Proposed system is simulated with the help of NS2 simulator. Evaluation of proposed system is done on the basis of various parameters like PDR, Delay and throughput. Performance of the proposed system is evaluated to be very high as compared to existing systems.

Keywords— MANET, Routing attack, Black hole attack, grey hole attack.

I. INTRODUCTION

A. MANET (Mobile Adhoc Network)

A Mobile Adhoc Network is a collection of mobile or wireless nodes. It is a decentralized network where nodes act as a router so that they can exchange the information with each other. Since the nodes can join and leave the network, hence the topology of the network is called dynamic topology. Because of this dynamic topology, network is more susceptible to several types of attacks. So it is very difficult for the network to develop a secure Adhoc routing protocol. MANET is always dealing with various types of attacks [1].Today Mobile Adhoc Network (MANET) is very popular. It is due to the need of communication between the mobiles nodes. As the popularity of the mobile network is increased, their security problems are also increased. These can damage the useful information to be communicated or drop it at all [2].

Fig 1.1 Mobile Adhoc Network

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

II. LITERATURE SURVEY

Vani A. Hiremani et al. in [1] implement a technique for co-operative blackhole and grayhole attacks and non consecutive co-operative blackhole and grayhole attack by using modified extended data routing information (MEDRI) table at each node with the routing table of the AODV protocol. This table records the information of malicious nodes.
Jyoti Rani et al. in [2] implement a approach to migrate the black hole attack using AOMDV (Ad hoc on Demand Multipath Distance Vector) routing protocol. This approach reduces the overhead.
Ms Monika Y. Dangore et al. in [3] discuss about the detection of blackhole attack and after detection of blackhole node it is bypassed and route to genuine destination is resumed again. The proposed approach shows the better network performance as compared to normal network.

Kriti Chadha and Sushma Jain in [4] discus about the routing protocols, security attacks such as active and passive attacks and effects of these attacks on applying ADOV protocol base on various performance metrics like throughput, packet drop ratio umber of dropped packets on parameters such as varying speed, number of nodes and pause time. Here the main focuses is on black hole attack and analyze its effect and the result shows that this attack has drastic effect the performance of the network and loss of packet is increased.

III. ATTACKS IN MANET

A. Types of attack in MANET

1) Denials of Services attack*:* This attack causes the problem in availability of a node or the effect the whole network. Node is not available when we required for transmission.

2) Impersonation: if the proper authority is not worked, than attacker node becomes a trusted node and sends the fake packet and accesses some secret data.

3) Eavesdropping**:** Node monitors the information and the information is used by attacker node, in information it may be some confidential location, password etc.

4) Routing attack- attacker node attack on the routing services. It attacks the routing protocols and delivery of packets**.**

5)Black hole attack **:** A malicious node sends false routing information, and claiming that it has best path for transmission. An attacker node drops all packets that it received from the other trusted nodes.

6) Wormhole attack**:** An attacker receives the packet at one location in the network, take them to another location in the network and send the answer from that location. And make a tunnel between two locations. This tunnel between two colluding attacks is known as a wormhole attack.

7) Man in middle attack**:** An attacker lies between the sender and receiver and sniffs any information that is being transmitted between nodes.

8) Gray hole attack*:* (routing misbehaviour attack)- it pretend itself as a trusted route and then drop the packets after a certain period of time-[5].

IV. METHODOLOGY

A. Proposed Algorithm for Detection and Prevention of Black hole Attack-

1) Detection :

Source node broadcast the RREQ to all its neighbor nodes.

1. Receive the RREP from neighbor nodes.
2. **S** predicts **D is** location and calculate **ERT** (expectedreplytime).
3. ERT increase according to distance between S and D.
4. If (M (malicious node) is present) then
   M sends immediately **RREP** to **S** and **S** compare **RREP** time with **ERT**
   Thus attacker is detected.

2) Prevention:

1. **S** set the timer expired for all **RREQ** store in CRRT in Seq. order.
2. CRRT Check which node repeatedly sends **RREP** to **S**.
3. If repeated hope count node value is present in CRRT.
   So the path is correct reply path. **M** has no hope count node it drop the **RREQ** packet toward **D**
   Else **M** is present.

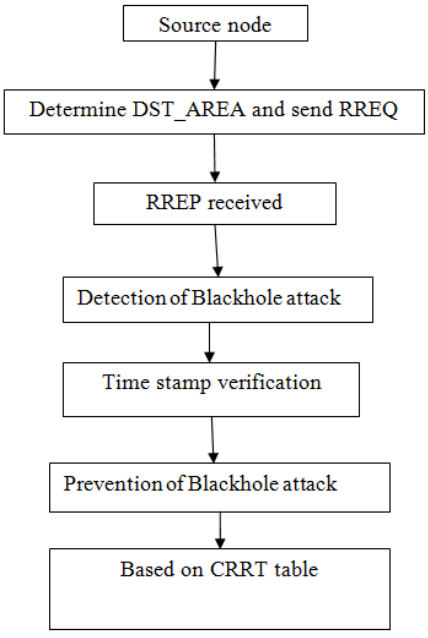

Fig.4.1 Block Diagram Prevention and detection of blackhole attack

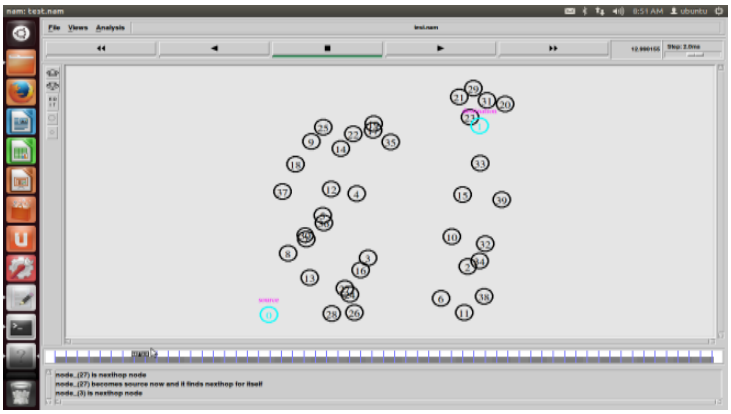

Fig 4.2 Source node broadcast the Request

In the above figure Source node sends the request to all the neighbour nodes and determines the shortest paths.

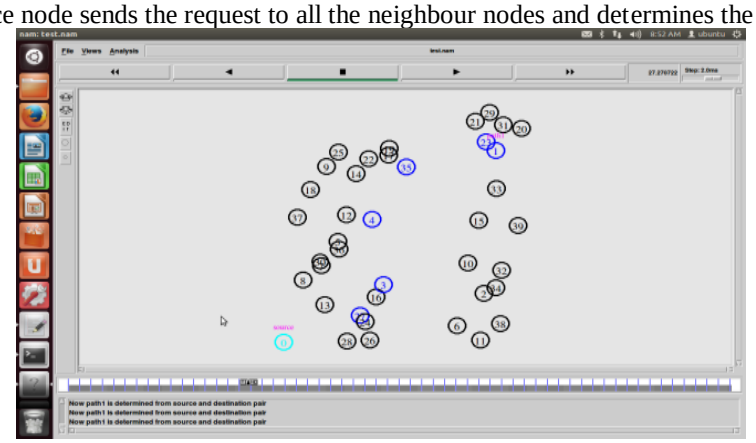

Fig 4.3 Identifying Path-I

In the above figure the first path is identified through 27-3-4-35-23 nodes with source as node 0 and the destination node 1.

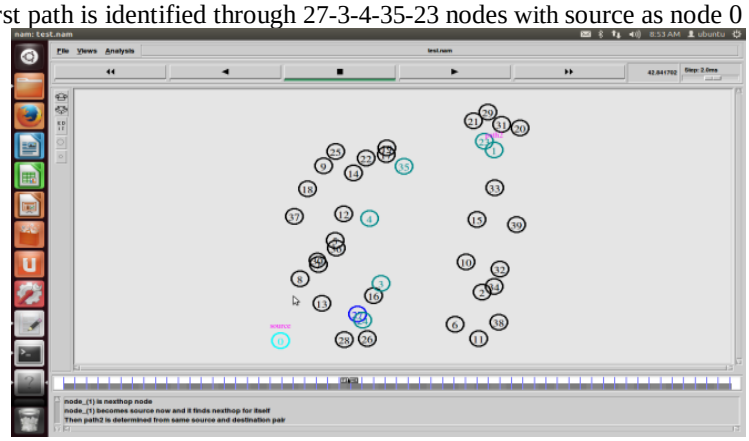

Fig 4.4 Identifying Path-II

In the above figure the second path is identified through 24-3-4-35-23 nodes with source as node 0 and the destination node 1.

Fig 4.5 Identifying Path-III

In the above figure the third path is identified through 8-12-35-23 nodes with source as node 0 and the destination node 1.

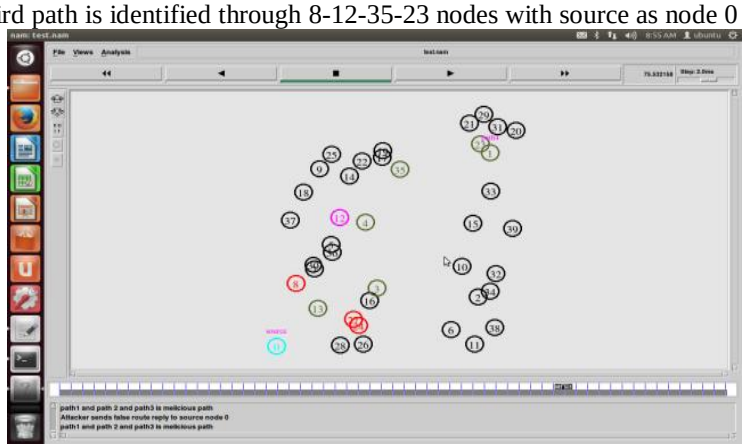

Fig 4.6 Identifying Path Malicious path

In the above figure source node sends route request to neighbour node. If attacker 8, 27, 24 is present in the network, immediately source is received the route reply from the attacker. After receiving RREP, source compares the RREP time with the expected RREP time. Source node 0 chooses the path which is not an attacker node. Data transmission occurs through 13-3-4-35-23-1 this path).

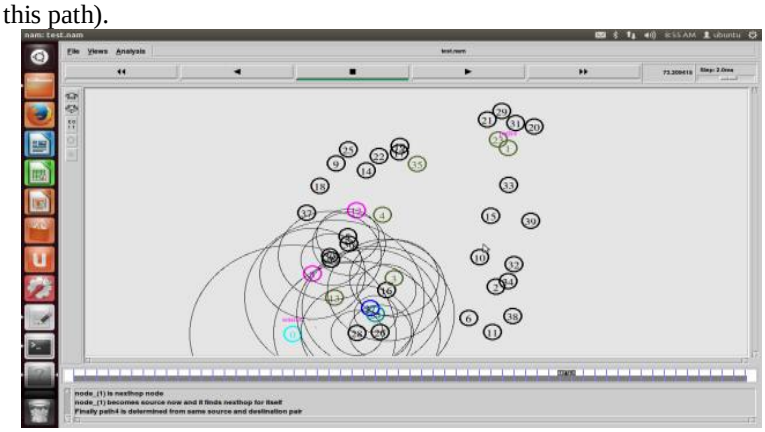

Fig 4.7Data transmission between source and Destination

In the above figure path 4 is determined from source and destination pair for data transmission.

V. ROUTING ATTACK

A. Procedure for Handling Routing Attack

1. Network Configuration and Initial Beacon Broadcast
2. Mobility Prediction (MP) Rule – (mobility dynamics)
3. On-Demand Learning (ODL) Rule – (forwarding patterns)
4. Mobility based forwarding node selection

1. Network Configuration and Initial Beacon Broadcast: Mobile Ad hoc network is created with the total number of 48 wireless nodes. Nodes are configured with simulation parameters listed in the simulation model table. Nodes are deployed in the initial location. After the deployment, each node identifies its neighbours by sending beacon. Nodes which are located within the communication range are known as neighbours. Each node broadcast the beacon to its neighbours.

2. Mobility Prediction (MP) Rule: The beacons transmitted by the nodes contain their current position and speed. Nodes estimate their positions periodically by employing linear kinematic equations based on the parameters announced in the last announced beacon. If the predicted location is different from the actual location, a new beacon is broadcast to inform the neighbours about changes in the node's mobility characteristics.

*3. On-Demand Learning (ODL) Rule***:** An accurate representation of the local topology is particularly desired at those nodes that are responsible for forwarding packets. Hence, APU seeks to increase the frequency of beacon updates at those nodes that overhear data packet transmissions. As a result, nodes involved in forwarding packets can build an enriched view of the local topology.

*4. Mobility based forwarding node selection (Highly stable Greedy forwarding)***:** In Mobile Adhoc Networks if forwarding nodes have high mobility may chances to make local topology inaccuracy. If the node involved in the forwarding path node moves frequently then there is the situation of frequent beacon update is required which leads to network traffic in turn packet collision. Hence it is required to select the nodes with low mobility which means selection of stable node as forwarder based on its mobility. This project with low mobility based forwarding node selection that improves routing performance more than APU.

Source node finds the distance of each neighbour from itself at particular time (t). After certain time (t+T) it finds the distance again. If the difference between the two distances is less than the threshold, the neighbour is considered as highly stable neighbour. To apply highly stable greedy forwarding distance between destination and highly stable neighbours are calculated. The neighbour which is having the minimum distance is selected as forwarder.

VI. RESULTS AND DISCUSSION

This chapter shows the results of simulation. We also evaluate the performance of the network by using AWK scripts. With the help of this script we obtain the performance of the network by various parameters.

A. Black hole Attack- Performance Metrics:

Following performance metrics capture the basic overall performance of the network.

1) End-to-End Delay: End-to-End delay is the time taken for a packet to reach the destination from the source node.

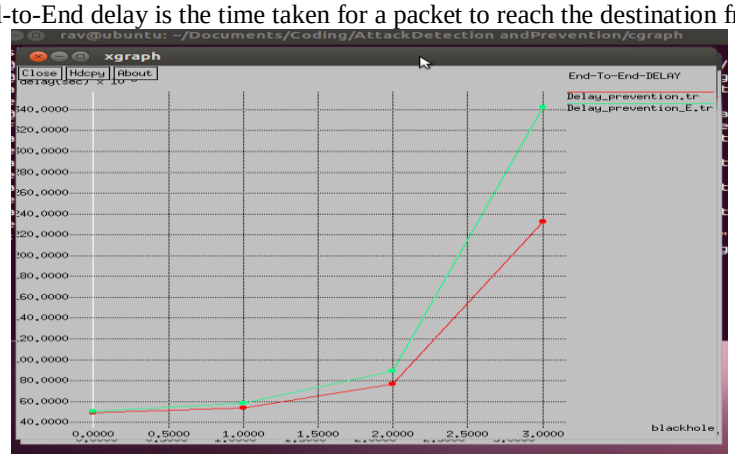

Fig 6.1 End to End Delay vs Blackhole 1, 2, 3

The figure 6.1 shows the End to End Delay in AODV (with Blackhole Attack) and without Blackhole Attack. Red line depicts the End to End Delay without Black hole attack whereas Green line depicts with the presence Black hole attack.

2) Throughput- No. of packet from source that a destination receive in a given time slot.

Fig 6.2 Throughput vs Blackhole 1, 2, 3

The figure 6.2 shows the throughput in AODV (with Blackhole Attack) and without Blackhole Attack. Red line depicts the Throughput without Black hole attack whereas Green line depicts with the presence Black hole attack.

3) Overhead- it is the ratio of routing packet sent and the total packet sent.

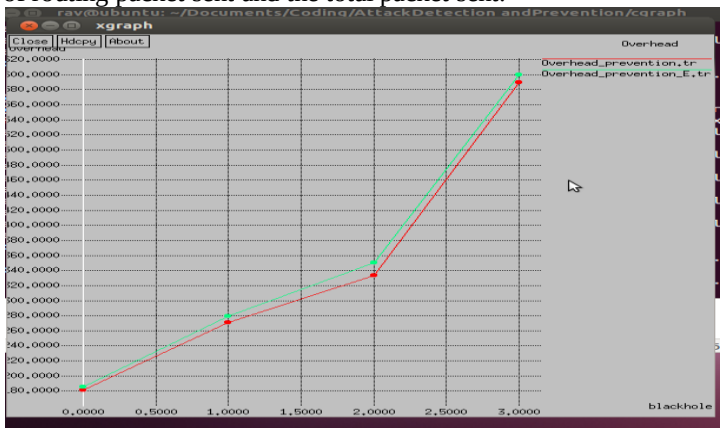

Fig 6.3 Overhead vs Blackhole 1,2,3

Figure 6.3 shows the Overhead in AODV (with Blackhole Attack) and without Blackhole Attack. Red line depicts the Overhead without Black hole attack whereas Green line depicts with the presence Black hole attack.

B. Routing Attack-

1) PDR (Packet Delivery ratio)- it is the proportion to the total amount of packets reached the receiver and amount of packet sent by source. If the amount of malicious node increases, PDR decreases. The higher mobility of nodes causes PDR to decrease.

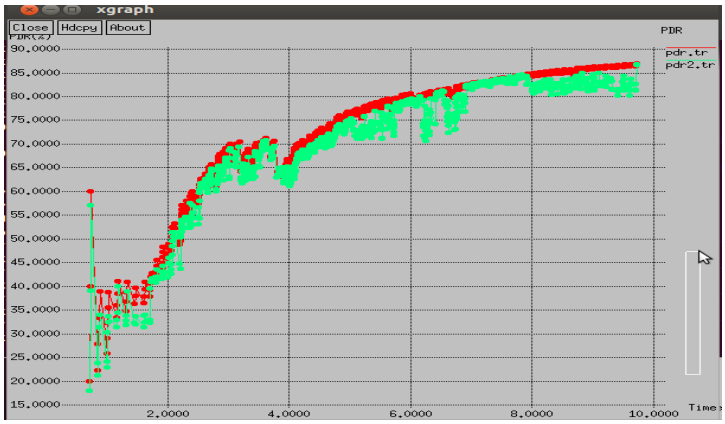

Fig 6.4 Packet delivery ratio vs time

Figure 6.4 shows the Packet Delivery Ratio in DSR protocol (with Existing periodic Base (PB) technique) and with our proposed Scheme (APU). Red line depicts the PDR with our proposed scheme whereas Green line depicts with existing PB scheme. As we can see when the time is increased PDR is also increased. In our proposed scheme PDR is higher than the existing PB scheme.

2) Energy Consumption: It is the amount of energy consumed by the sensors for the data transmission over the network

Energy Consumption = Sum of energy consumed by each sensor

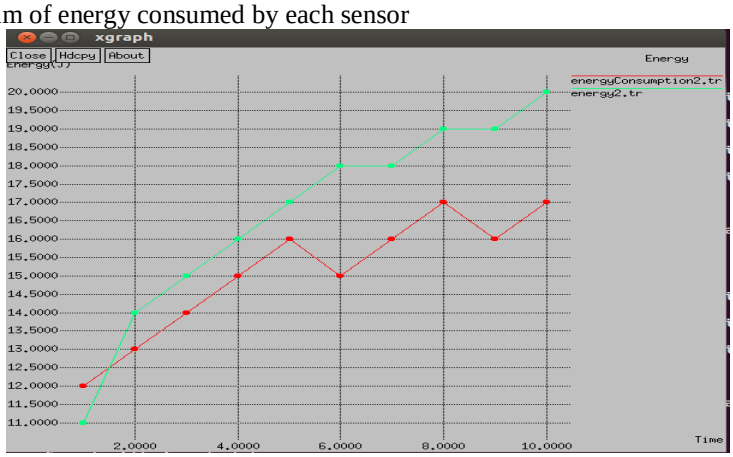

Fig 6.5 Energy Consumption vs time

The figure 6.5 shows the Energy consumption in DSR protocol (with Existing periodic Base (PB) technique) and with our proposed Scheme (APU). Red line depicts the Energy consumption with our proposed scheme whereas Green line depicts with existing PB scheme. As we can see when the time is increased Energy consumption is also increased. In our proposed scheme Energy consumption is less than the existing PB scheme

3) Overhead: Number of messages involved in beacon update process

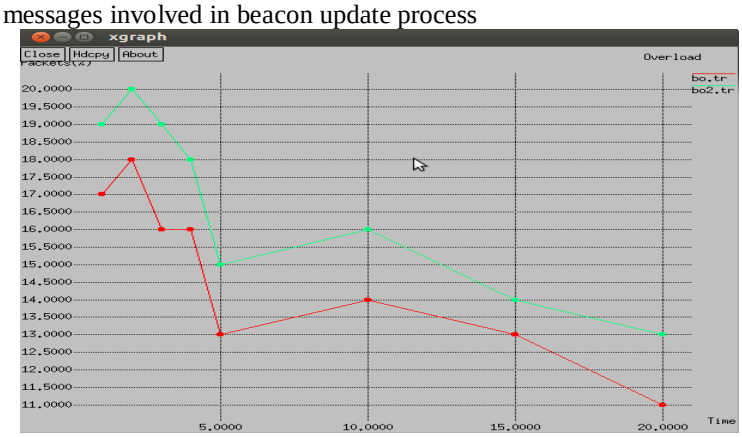

Fig 6.6 Beacon overhead vs time

The figure 6.6 shows the beacon overhead with existing technique (Green line) and our proposed scheme (red line) In our proposed scheme overhead is less than the existing PB scheme.

VII. CONCLUSION AND FUTURE SCOPE

MANET is a collection of mobile or wireless nodes. After studied the various types of attacks and techniques in MANET for evaluating the performance of network which suffering from blackhole attack. Our proposed work includes the detection and prevention mechanism for black hole attack in MANET by using AODV routing protocol. This shows the better network performance in terms of throughput, end to end delay and overhead. For routing attack (Packet collision) we propose the mechanisms which regularly update the node location information by using APU (Adaptive Position Update) scheme. Simulation results show the better overhead, packet delivery ratio and energy consumption than the existing scheme.

In future work it can be further evaluated by taking the other performance parameters (no. of nodes, first node failure time, dropped packet information etc.) against these attacks and also evaluate the performance of other attacks.

REFERENCES

[1] Vani A. Hiremani, ME (Comp.) and Manisha Madhukar Jadhao "Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET" (IEEE)International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)pp-944-948,2013.

[2] Jyoti Rani and Naresh Kumar "Improving AOMDV Protocol for Black Hole Detection in Mobile Ad hoc Network "(IEEE) International Conference on Control, Computing, Communication and Materials (ICCCCM), 2013.

[3] Ms Monika Y. Dangore and Mr Santosh S. Sambare "Detecting and Overcoming Blackhole Attack in Aodv Protocol" 2013(IEEE) International Conference on Cloud & Ubiquitous Computing & Emerging Technologies pp.77-82, 2013.

[4] Dr. Sushma Jain and Kriti Chadha "Impact Of Black Hole And Gray Hole Attack In AODV Protocol" IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, India, May 09-11, 2014.

[5] Priyanka Goyal, Vinti Parmar and Rahul Rishi "MANET: Vulnerabilities, Challenges, Attacks, Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, pp. 32-37, January 2011.

[6] Pramod Kumar Singh and Govind Sharma "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", proceedings of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, pp. 902-906, 2012.

[7] Harsh Pratap Singh and Rashmi Singh "A Mechanism for Discovery and Prevention of Cooperative Black hole attack in Mobile Ad hoc Network Using AODV Protocol"

[8] 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, pp.88-93, August 2012.

[9] Nitesh A. Funde1, P. R. Pardhi "Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET" International Journal of Advanced Research in Computer and Communication Engineering Volume-2, Issue -10, pp.4132-4136, October 2013.

[10] K. Lakshmi, S.Manju Priya, A.Jeevarathinam , K.Rama,and K. Thilagam" Modified AODV Protocol against Blackhole Attacks in MANET" International Journal of Engineering and Technology Volume-2 , Issue -6, pp.444-449, 2010.

[11] Ms. Gayatri Wahane and Ms. Savita Lonare "Technique for Detection of Cooperative Black Hole Attack in MANET". IEEE-31661, 4th ICCCNT, July 4-6, 2013.

[12] P.Gowrisankar, N.Srinivasulu and Dr.Ch.Balaswamy "Design and Implementation of Black-hole Attacks in AODV Routing Protocol for Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering, Volume- 2, Issue-12, pp.4548-4554, December 2013.

[13] Nisha, Simranjeet Kaur and Sandeep Arora "Analysis Of Black Hole And Gray Hole Attack On RP-AODV In MANET" International Journal of Engineering Research & Technology (IJERT)Volume-2 Issue- 8, pp.193-196, August – 2013.

