IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Cooperative Black Hole Attack Prevention by Particle Swarm Optimization

Shivani[1], Pooja Rani[2]

Student, Department of Computer Science & Engineering, Rayat & Bahra, Mohali, India[1]

Associate Professor, Department of Computer Science & Engineering, Rayat & Bahra, Mohali, India[2]

Abstract: A Mobile ad hoc network is a infrastructure less network in which nodes change their positions dynamically. Some features of MANET like Dynamic topology, Lack of centralized management, Scalability etc. make it more vulnerable to attacks. Black hole is one of the possible attacks that occur in the network as advertising itself having the shortest path to the destination node in the network. Thus it seeks the attention of source node to itself and takes part in communication. When number of malicious nodes work together, it is called cooperative black hole attack. In this paper, we are analyzing the AODV protocol with PSO (Particle Swarm Optimization) technique to find solution for multiple attacker nodes in the network. Particle Swarm Optimization monitors nodes by changing their values because of ad hoc nature, if node converge then it change node's value to infinite and prevent the node to send packet. The simulation is performed on the basis of different performance parameters like Throughput, End to End Delay and Drop Packet.

Keywords: Cooperative Black hole Attack, AODV Routing Protocol, Throughput, End to End Delay, Drop Packet

I. INTRODUCTION

A mobile Ad hoc network (MANET) is a infrastructure less network and it is a self configuring network. A MANET is a collection of wireless mobile nodes that communicate with each other without the use of a centralized administration or any network infrastructure. The mobile nodes in the network are not bound to any centralized control like base stations [1].

In an ordinary wireless network, two nodes cannot communicate with each other when the distance between the two nodes is beyond the transmission range. MANET solves this problem by allowing intermediate nodes to relay data transmissions. In MANET, mobile nodes can act as both routers and hosts. It work on dynamic topology where nodes may join and leave the network at any time with their own choice and the multi-hop routing may keep changing as nodes join and depart from the network. In this paper, we used the PSO (Particle Swarm Optimization) technique for solving the problem of Cooperative Black Hole attack. We analyzed the vulnerability of AODV routing protocol with PSO technique for preventing the black hole nodes.

1.1 Black hole Problem in MANET

A black hole problem means that a malicious node utilize the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. As shown in figure 1.1, Source node 'A' broadcasts a RREQ packet to make a communication with the destination node 'H', nodes 'B' 'D' and 'B1' receive it [4]. Node 'B1', being a malicious node, immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'B1' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'B1' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'B1', it absorbs all the data and thus behaves like a 'Black hole'. Also 'B2' is another black hole node and when they perform attack cooperatively, it is known as cooperative black hole attack.

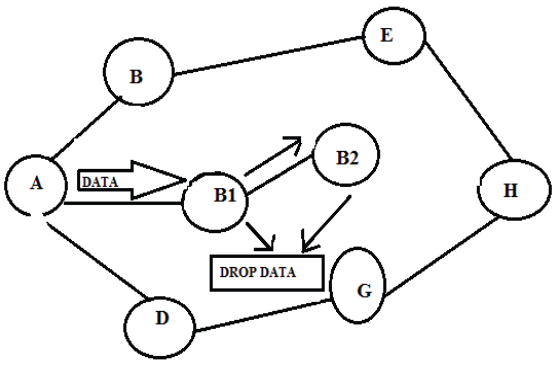

Figure 1.1 Cooperative Black hole Problem in MANET [4]

1.3 PSO (Particle Swarm Optimization)

Particle Swarm Optimization is a search algorithm that has been inspired from bird flocking and fish schooling. It uses a number of agents (particles) that constitute a swarm moving around in the search space looking for the best solution. Here we use this technique for optimizing the values of nodes globally. The values are optimized by PSO by converging them on the basis of the shortest path of nodes in the network. The attacker nodes are detected

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

with the help of this optimization technique. Because the value of the attacker node will never change, so it becomes easy to detect the malicious node with the help of this technique.

1.4 AODV Routing Protocol

The Routing operation of AODV is a two stage process.
In AODV when a node wants to communicate with other node in the network which is not directly in its transmission range, it checks for a route in routing table for that particular node. If no entry is found in the routing table, Node broadcast route request message (RREQ) in network. Nodes that receive that route request checks for the destination node route in their routing table. If the fresh route is found, it unicast the Route Reply Packet (RREP) to source, else in the case of no route it rebroadcast the request in network. Once the source receives the RREP, it starts sending data packets [10].
Route maintenance occurs when there is a link break due to changing topology of the network. Due to the random node movement frequent link break occurs. When a node detects a link break, it sends a Route Error (RERR) packet to the corresponding routing table, which then removes all the entries with compromised route in the routing table.

II. LITERATURE REVIEW

Deng et. al [1], proposed a technique for detecting a chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc networks. The optimality of backbone network is not proved in terms of minimality and coverage. The assumption that strong nodes are always trusted node will fail if the intruder attacks strong nodes.
Tan & Kim [2], proposed a mechanism that provides Secure Route Discovery for the AODV protocol (SRD-AODV) in order to prevent Black Hole attacks. The simulation results showed that SRD-AODV mechanism greatly increases the packet delivery ratio for three types of environments with node mobility when Black Hole attacks are occurring on the network. Narayanan & Radhakrishnan [3], presented a defense mechanism against Black Hole attacks in MANET. This method makes use of the MAC address of the destination to validate each node in its path thereby providing a direct negotiation for secure route. Packet delivery ratio and throughput of secure AODV with respect to pause time and mobility is always higher than AODV with Black Hole attack. Anishi Gupta [8], proposed a new method RTMAODV (Real Time Monitoring AODV). Moreover neighbor node detects and prevents Black Hole attack using real time monitoring. The concept of broadcasting is being used in the method. In simulation, new method has shown outstanding result in terms of packet delivery ratio as compare to AODV routing protocol in presence of malicious node under Black Hole attack.
Ranjan et. al [9], have focused on the Black Hole attacks. AODV (Ad hoc on demand Distance Vector) routing being one of the many protocols often becomes an easy victim to such attacks. Besides the security issues they also described the layered architecture of MANET, their applications and a brief summary of the proposed works that have been done in this area to secure the network from Black Hole attacks.

III. PROPOSED WORK

In the proposed system, we are preventing cooperative black hole attack in the network. In this multiple attacker nodes are there in the network. These attacker nodes are prevented by Particle Swarm Optimization technique. This technique prevents the malicious nodes by optimizing them. In proposed work some steps have been taken. MANET scenario will be generated which will be generated with the help of network simulator NS2.

Algorithm Steps:
Step 1: Deploy the wireless nodes in one-thousand X one-thousand.
Step 2: Set the mobility of the nodes and set the packet distribution parameter with First Come First Serve method.
Step 3: Stimulate the attack on more than one node and analyze the throughput, End to End Delay and drop packet.
Step 4: Initialization of prevention of attack by Particle Swarm Optimization and initialize the swarm which depend on number of nodes.
Step 5: Optimize the shortest path value of every node if it will change then, it's a genuine node, otherwise attacker node.
Step 6: After identifying the attacker node, set the shortest path value of these nodes infinite.
Step 7: Analyze the throughput, End to End Delay and drop packet in different set of nodes.

IV. RESULTS & DISCUSSIONS

4.1 Simulation:

The proposed technique is simulated using network simulator NS2. In this, AODV protocol and the proposed scheme are simulated and these are also compared on the basis of certain parameter metrics (End to End Delay, Throughput and Drop Packet). The simulation parameters for the simulations are shown in the following table 4.1:

Table 4.1 Simulation Parameter for Analysis

PARAMETER	VALUE
No. of nodes	20,30,50,80
Simulation Area	1000m*1000m
Simulation Time	600 sec
Speed	30m/s
Mobility Model	Random Walk
Traffic/connections	TCP
MAC Protocol	802.11
Transmission Range	150m
Protocol	AODV

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

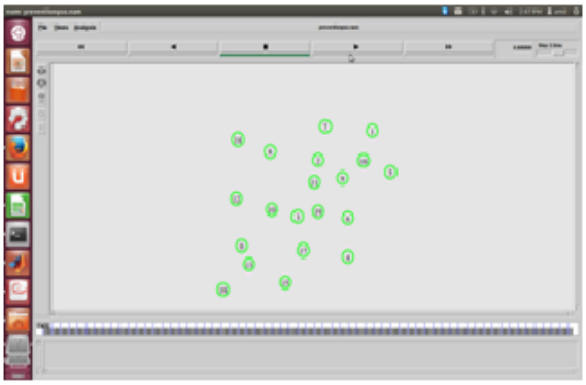

Figure 4.1: Initialization of nodes

This figure 4.1 shows the initialization of different nodes in the mobile Ad hoc network. There are 20 nodes in the network.

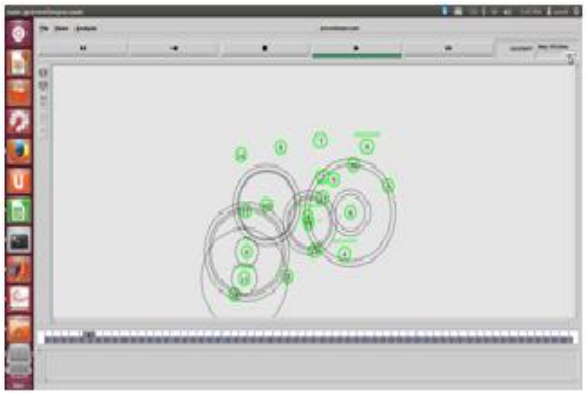

Figure 4.2: Starting of simulation of nodes

In figure 4.2 the source node sends the route request packet to all its neighbors in the network to find the route to the destination. Also the attacker nodes have been introduced to the network having shortest path values. As the source node get the replies from various neighbor nodes, it starts sending data packets to the route having shortest path. Then the performances of parameters that are Throughput, End to End Delay and Drop Packet have been measured. Because of the attacker nodes the packets sent by source node have been dropped which degraded the network performance.

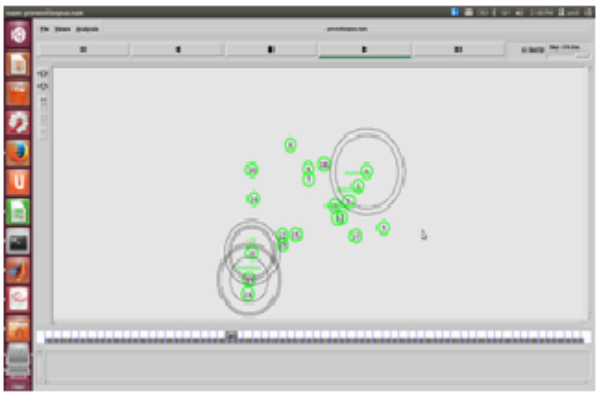

Figure 4.3: Sending Data Packets

In figure 4.3, as the source node get the replies from various neighbor nodes, it starts sending data packets to the route having shortest path. Then the performances of parameters that are Throughput, End to End Delay and Drop Packet have been measured. Because of the attacker nodes the packets sent by source node have been dropped which degraded the network performance.

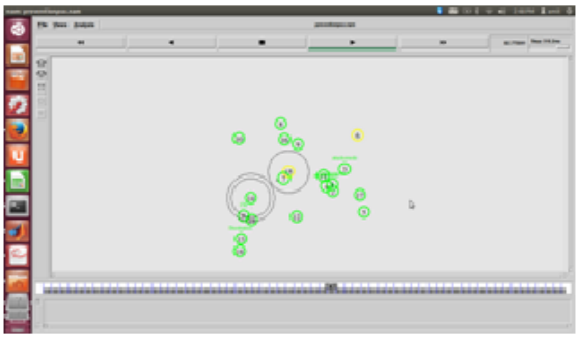

Figure 4.4: Applying PSO

This figure 4.4 shows the working of PSO (particle swarm optimization) technique. This technique starts preventing the network from multiple attacker nodes. Here the yellow nodes are taken as the predicted attacker nodes which are to be prevented by PSO.

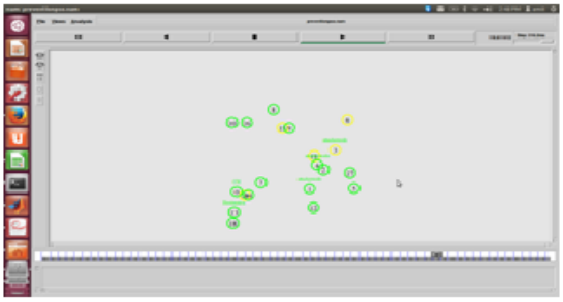

Figure 4.5: Prevention of Predicted Nodes

This figure 4.5 Particle Swarm Optimization takes the shortest path values of the nodes which makes route replies. Then it converge the values of those nodes. If the value of any node is not changed then that node is taken as the attacker node. Thus PSO detects the attacker nodes. After that PSO sets the value of attacker node to infinite. The yellow node 3, node 6, node 11, node 15 and node 19 are the prevented nodes.

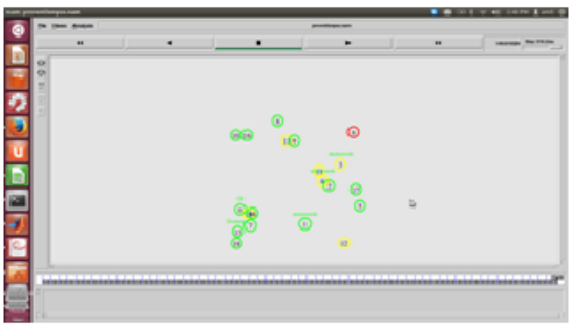

Figure 4.6: Prevented node with optimization

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

In figure 6.6, the node 6 is the highly prevented attacker node and prevented from the network. The node 6 is the node which is the highly attacking node and that is prevented with optimization by particle swarm optimization technique.

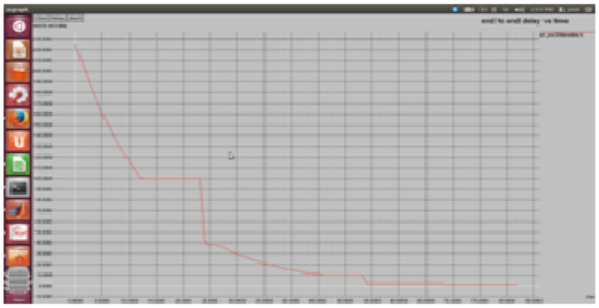

Figure 4.7: End to End Delay

Figure 4.7 shows the simulation graph of End to End Delay.

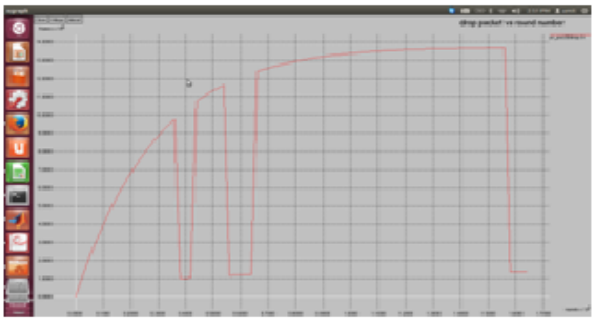

Figure 4.8: drop packet

Figure 4.8 shows the simulation graph of drop packet

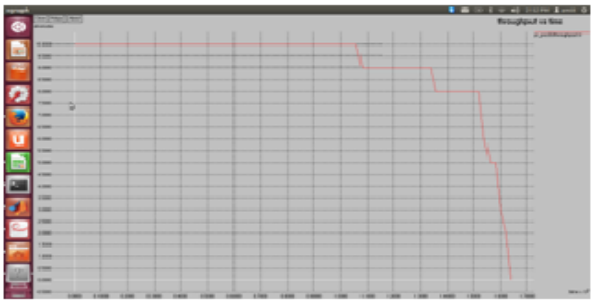

Figure 4.9: Throughput

Figure 4.9 shows the simulation graph of Throughput.

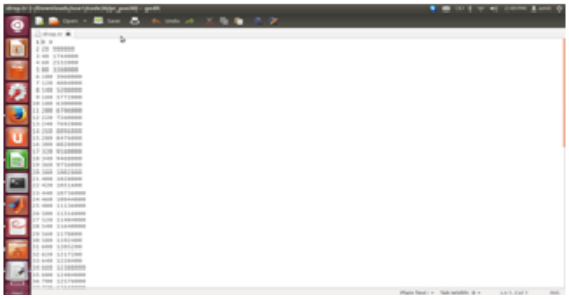

Figure 4.10: Trace file of Drop Packet

Figure 4.10 shows the trace file of Drop Packet which is generated by simulation graph of drop packet.

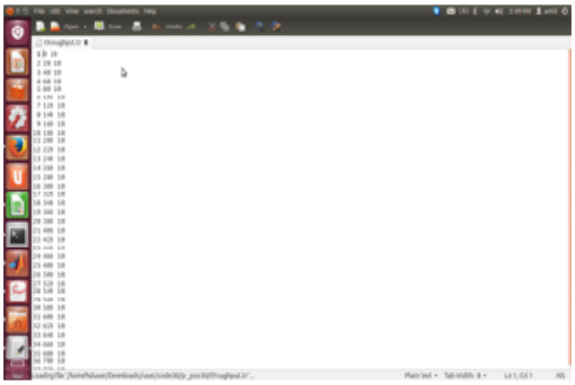

Figure 4.11: Trace file of Throughput

Figure 4.11 shows the trace file of Throughput which is generated by simulation graph of Throughput.

Figure 4.12: Trace file of End to End Delay

Figure 4.12 shows the trace file of End to End Delay which is generated by simulation graph of End to End Delay.

4.2 Results and Analysis: The following metrics are used to analyze the simulation results.

4.2.1 Throughput: It is the rate of successfully transmitted data packets in a unit time in the network during the simulation.

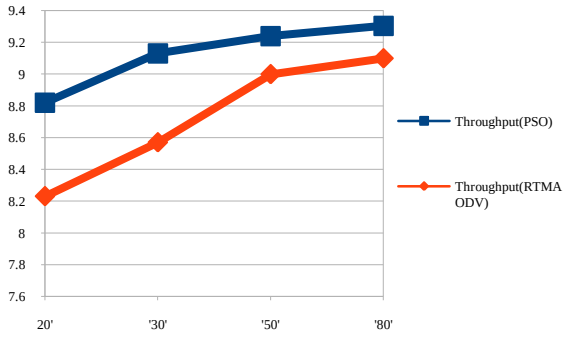

Figure 4.13: Representation of Throughput

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Figure 4.13 shows the graph of comparison between throughput (PSO) and throughput (RTMAODV). The proposed technique gives better results than the existing technique. The proposed technique increases the throughput as compared to the existing technique.

4.2.2 End to End Delay: This metric indicates how long it takes for a packet to travel from the source to the destination. This includes all the delays caused by buffering during route discovery, processing at intermediate nodes, retransmission delays, propagation and transfer times. It is measured in milliseconds.

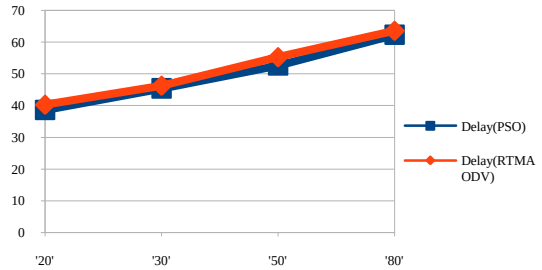

Figure 4.14: Representation of End to End Delay

The figure 4.14 shows the graph of comparison between End to End Delay (PSO) and End to End Delay (RTMAODV). The proposed technique decreases the End to End Delay of data packets as compared to the existing technique.

4.2.3 Drop Packet: Packet drop occurs when one or more packets of data travelling across a computer network fail to reach their destination.

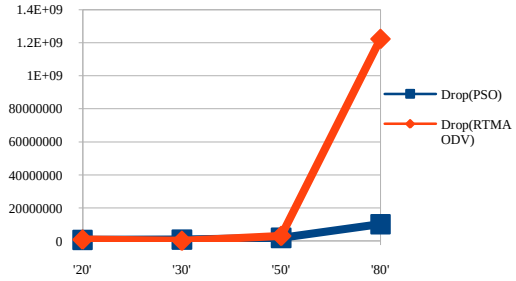

Figure 4.15: Representation of Drop Packet

The figure 4.15 shows the graph of comparison between Drop Packet (PSO) and Drop Packet (RTMAODV). The proposed technique gives better results than the existing technique. The proposed technique decreases the no. of dropped packets as compared to the existing technique.

V. CONCLUSION

Mobile ad hoc network has still many challenges left in order to overcome with the importance of MANET comparative to its vast potential. In our paper we have analyzed the behavior and challenges of security attacks in mobile ad hoc networks with solution finding technique. In our stud y we analyzed cooperative Black Hole attack with four different scenarios with respect to the performance parameters Throughput, End to End Delay and Drop Packet. We have analyzed the vulnerability of protocol AODV with PSO (Particle Swarm Optimization) and this technique give better results than RTMAODV technique. We tried to discover and analyzed the impact of Cooperative Black Hole attack in MANETs using AODV protocol. In future Black Hole attack can be analyzed in other MANETs routing protocols such as OLSR, DSR, TORA and GRP etc. Other types of attacks such as Jellyfish, Sybil and Wormhole attacks are needed to be studied in comparison with Black Hole attack.

ACKNOWLEDGEMENT

I want to thank almighty who guided me throughout the way. Apart from this, I want to thank and express my deepest gratitude and regards to my guide **Er. Pooja Rani** (Associate Professor) for her full support and expert guidance throughout my study and research.

REFERENCES

[1] Hongmei Deng, Wei Li and Dharma P. Agrawal, “Routing Security in Wireless Ad hoc Networks”, IEEE Communications Magazine Journal, Vol. 40(10), pp. 70-75, 2002.

[2] Seryvuth Tan and Keecheon Kim, “Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs”, High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on, pp. 1159-1164. IEEE, 2013.

[3] S. Sankar Narayanan, and S. Radhakrishnan, “Secure AODV to Combat Black Hole Attack in MANET”, Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, pp. 447-452. IEEE, 2013.

[4] Vani A. Hiremani, and Manisha Madhukar Jadhao, “Eliminating Co-operative Black Hole and Gray Hole Attacks using Modified EDRI Table in MANET”, Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on, pp. 944-948. IEEE, 2013.

[5] Amara Korba Abdelaziz, N. Mehdi, and G. Salim, “Analysis of Security Attacks in AODV”, International Conference on Multimedia Computing and Systems (ICMCS), 2014.

[6] Martin K. Parmar, and Harikrishna B. Jethva “Analyse Impact of Malicious Behaviour of AODV under Performance Parameters”, Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, pp. 719-724. IEEE, 2014.

[7] Ankit D. Patel, and Kartik Chawda, “Black Hole and Gray Hole Attacks in MANET”, In Information Communication and Embedded Systems (ICICES), 2014 International Conference on, pp. 1-6. IEEE, 2014.

[8] Anishi Gupta, “Mitigation algorithm against Black Hole Attack Using Real Time Monitoring for AODV Routing Protocol in MANET”,Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, pp. 134-138. IEEE, 2015.

[9] Rakesh Ranjan, Nirnemesh Kumar Singh, and Ajay Singh, “Security Issues of Black Hole Attacks in MANET”, Computing, Communication & Automation (ICCCA), 2015 International Conference on, pp. 452-457. IEEE, 2015.

[10] Sakshi Jain, Dr. Ajay Khuteta, “Detecting and Overcoming Black Hole Attack in Mobile Ad hoc Network”, International Conference on Green Computing and Internet of Things (ICGCIoT). IEEE 2015.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

BIOGRAPHIES

Shivani is pursuing Masters of Technology in Computer Science Engineering from Rayat & Bahra College Mohali, Punjab (India). She received the degree of Bachelor of Technology in Computer Science Engineering from Shobhit University Meerut, UP (India). Her area of interest is Mobile Ad hoc Network.

Pooja Rani received her M.Tech. degree and also pursuing Ph.D. in computer engineering. She has 10 years of teaching experience. Presently she is working as Associate Professor in Rayat & Bahra College of Engineering & Biotechnology, Mohali, Punjab.