

Black Hole Attack in Mobile Ad-Hoc Network

Avinash Kamal Mishra¹ Hina Rabbani²

¹M.Tech Student ²Assistant Professor

^{1,2}Department of Computer Science & Engineering

^{1,2}BBD University, Lucknow, India

Abstract— The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviours because the route discovery process is necessary and inevitable. An assortment of attacks is there to mischief the dexterous working of MANET. One of these attacks is the Black Hole attack which leads to dropping of messages. Attacking node leading agrees to forward packets and then not succeeded to do so. Black Hole attack may take place due to a malicious node which is consciously misbehaving as well as a smashed node interface. In any case, nodes in the network will continuously trying to find a route for the destination, which makes the node consume its battery in addition to losing packets. In this paper we analyse Black Hole attack in MANETs using AODV and OLSR which are reactive and proactive respectively in nature.

Key words: MANET, Black Hole Attack, Security Threats, AODV Protocol

I. INTRODUCTION

Wireless networks use some kind of radio frequencies in air to transmit and receive data instead of using some physical cables. Wireless networks are formed by routers and hosts. Ad-hoc networks are wireless networks, in which nodes communicate with each other using multi-hop links. Network which support wireless architecture are known as mobile Adhoc Network [1]. Such networks can be used to enable next generation battlefield applications, including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. MANETs have some exceptional characteristic features such as undependable wireless media (links) used for communication flanked by hosts, determinedly changing network topologies and memberships, inadequate bandwidth, battery, existence, and working out power of nodes etc. Ad hoc networks make available a prospect of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with predetermined infrastructure, mobile nodes in ad hoc networks do not communicate by means of access points. Every mobile node operates as a host when requesting/providing information from/to other nodes in the network, and acts as router when ascertaining and maintaining routes for other nodes in the network [2].

The dynamic nature of ad hoc networks requires that prevention techniques should be complemented by detection techniques, which scrutinize security condition of the network and identify malicious behavior. One of the most decisive predicaments in MANETs is the sanctuary vulnerabilities of the routing protocols. A set of nodes in a MANET may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and

flood other nodes with routing traffic. An OADV is a source initiated on-demand routing protocol. On the other hand, AODV [3] is susceptible to the well-recognized black hole attack. In black hole attack an attacker node transmits infected packet to an unknown receiver. When a node receives it gets infected and behaves like malicious node and transmitted multiple of reflected packets to others and same procedure used to infect the whole network. The Black Hole attack [4, 5] is a class of denial of service where a malevolent node can magnetize all packets by untrustworthily claiming a fresh route to the target and then saturate up them devoid of forwarding them to the target. Cooperative Black hole means the malicious nodes operate in a group [6].

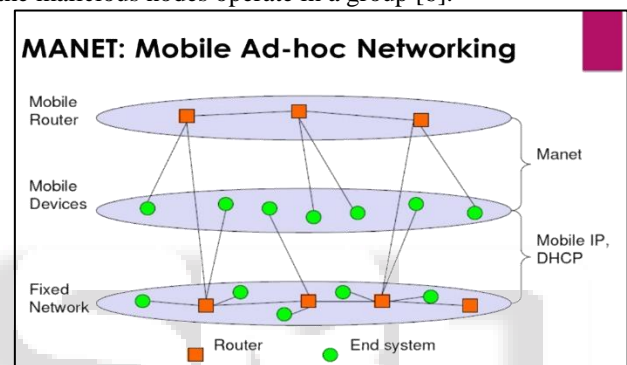


Fig. 1:

The remaining part of the paper is prearranged as follows: In section II discusses black hole in AODV routing overview. The Section III presents the literature of previous work done and last section presents conclusion of the paper.

II. AODV ROUTING PROTOCOL

AODV is distance vector routing protocol that establishes route to the destination when it is desired by the source node. It sustains these routes as and when desirable by the source node. It offers quick adaptation to self-motivated link conditions, low processing, memory overhead, low network deployment, and establishes unicast routes to destinations within the ad hoc network [3]. One of the distinctive features of AODV protocol is its use of destination sequence number associated with all route. Destination sequence number is created by the destination to include route information about it send to the requesting node. In order to correspond amongst the mobile nodes, [3] Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. When a source node desires to attach to a destination node, primary it checks in the presented route table, as to whether a fresh route to that target is existing or not. New adequate route means a valid route entry whose sequence number is larger than it in the RREQ. Larger the sequence number, fresher is the route. If a new adequate route is presented, it uses the same. If not, the node initiates a Route innovation by broadcasting a RREQ control message to all of its neighbors.

This RREP message will additionally forwarded by the intermediate nodes to their neighbors having a new route to the target. The RREQ message will ultimately reach the target node, which will respond with a route reply message (RREP). The RREP is sent as a unicast to the source node beside the overturn route established during the RREQ broadcast. Likewise, the RREP message allows intermediary nodes to learn a forward route to the target node. Therefore, at the end of the route discovery process, packets can be delivered from the source node to the target node and vice versa. A route error message (RERR) allows nodes to notify errors due to link breakage, such as when a preceding neighbor moves to a novel position and is no longer accessible. Each mobile node would periodically send Hello messages (HELLO), consequently, every one node knows which nodes are its neighboring nodes. AODV as a reactive routing protocol does not provide nodes an absolute view of network topology. That is, every node only knows its neighbors, and for the non-neighbors, it simply knows the next hop to reach them and the distance in hops. However, the security of AODV is conciliated by the Black Hole nodes, as it acknowledges the received RREP having fresher route. The standard AODV routing protocol cannot fight the threat of Black Hole attacks, because during the phase of route detection, malicious nodes may forged a sequence number and hop count in the routing message; In this manner, obtaining the route [15], eavesdropping and plummeting all the data packets as they pass or forward some discriminating packets to the destination.

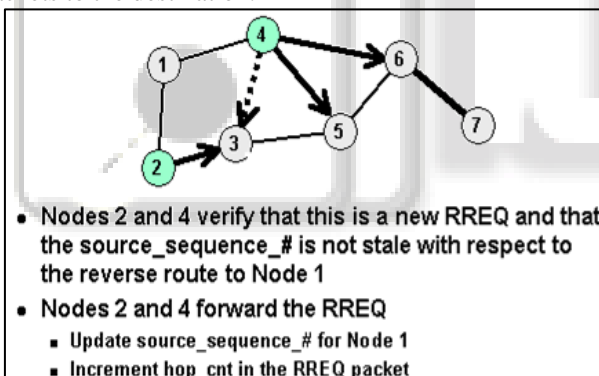


Fig. 2: Working of AODV Protocol

III. BLACK HOLE ATTACK IN AODV

The attacks in mobile ad hoc network are classified into two categories: one is active attack and another is passive attack. The black hole attack is an example of active attack; it can be a single black hole or cooperative black hole. In Mobile Ad hoc Network a packet plummet attack or black hole attack is a diversity of denial-of-service attack in which a router that is thought to impart packets instead discards them [4]. This typically takes places from a router becoming compromised from a number of dissimilar causes. One cause declared in investigation is during a denial-of service attack on the router using a known DoS tool. For the reason that packets are routinely plummeted from a lossy network, the packet drop attack is dreadfully hard to identify and thwart. Node 4 shows the malicious node in the figure 3 operate with each other.

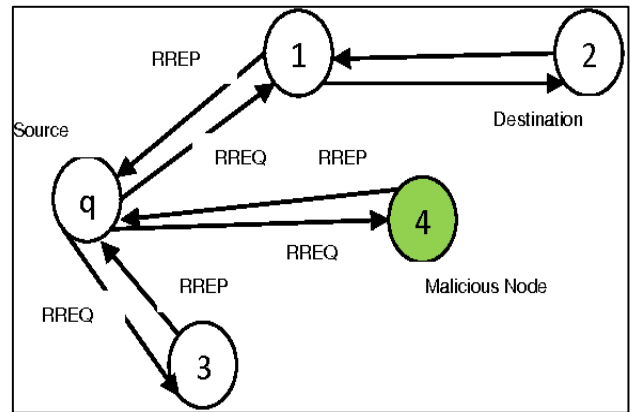


Fig. 3: Single Black Hole Node in AODV Protocol

The cooperative black hole is a type of attack in which black hole nodes act in a group together [7]. For example when multiple black hole nodes are acting in coordination with each other, the first black hole node refers to the one of its teammate in the next hop. This type of attack harms the system very much and affect the throughput of the system. The nodes 1, 4 and 6 in the following figure are malicious nodes that act in coordination with each other.

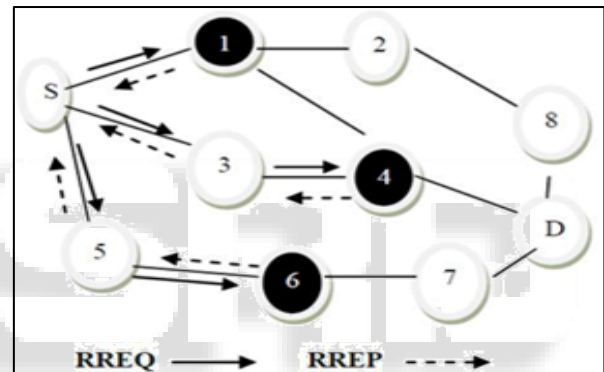


Fig. 4: Cooperative black hole node in AODV protocol [7]

IV. RELATED WORK

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks [4, 9]. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [9, 21]. Different kinds of attacks have been analyzed in MANET and their effect on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [14]. MANETs routing protocols are also being exploited by the attackers in the form of flooding attack, which is done by the attacker either by using RREQ or data flooding [16].

In any network, the sender wants its data to be sent as soon as possible in a secure and fast way, many attackers advertise themselves to have the shortest and high bandwidth available for the transmission such as in wormhole attack, and the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes [12, 17]. One of the most arising issues in MANET is the limited battery, attackers take an advantage of this flaw and tries to keep the nodes awake

until all its energy is lost and the node go into permanent sleep [18]. Many other attacks MANET such as jellyfish attack, modification attack, misrouting attack and Routing Table Overflow have been studied and exposed [19, 13, and 20].

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [23, 24]. In [3] a path based detection method is proposed, in which every node is not supposed to watch every other node in their neighborhood, but in the current route path it only observes the next hop. There is no overhead of sending extra control packets for detecting Black Hole attack.

Many solutions have been proposed to combat on Black Hole attack, one of the solution proposed by Deng gives the approach of disabling the reply message by the intermediate. This method avoid intermediate node to reply which avoid in certain case the Black Hole and implements the secure protocol.

The solution proposed in focus on the requirement of a source node to wait unless the arrival of RREP packet from more than two nodes. When it receives multiple RREPs the source node check that there is any share hops or not. The source node will consider the routed safe if it finds the share hops. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of node.

V. RESULT ANALYSIS

The last stage is important and most of the time was given to this stage. We analyzed the behavior of system under attack (in presence of black hole attack) and compare it to the system with no attack (i.e. normal working protocol). All the results obtained from simulation are analyzed carefully and the simulation is run for several times for different time interval in order to get a stabilized reading. Once the systems get stabilized the results are analyzed and on the basis of analysis, conclusions are drawn.

VI. SIMULATION TOOL

OPNET tool is selected to carry out the simulation. All of the simulation is carried out in OPNET modeler 14.5. OPNET provide technologies, protocols, communication devices for academic research, assessment and improvement. It is efficient, robust and highly reliable and as it was available for us in our labs so it was the obvious choice for us to select the appropriate simulation tool.

VII. PERFORMANCE PARAMETERS

Three performance parameters i.e. end to end delay; throughput and network load is taken. Our aim was to study the effect of black hole on AODV and OLSR by analyzing that how much performance of a network has been compromised in other words these parameters show us extend of vulnerability of black hole attack of selected network protocol (AODV, OLSR). It is important to take into

consideration of reader that the delay is taken in term of whole network and then its performance in the presence of a single black hole node is analyzed. Similarly performance parameters i.e. throughput and network load shows to the extent of network performance has been affected by the presence of black hole node.

VIII. PERFORMANCE ANALYSIS

This chapter explains the various performance metrics required for evaluation of protocols. To reiterate the black hole attack, we begin with the overview of performance metrics that includes End-to-end delay, Throughput and Network load. These matrices are important because of it performance analysis of network. Furthermore, implementation of the simulation setup, tools and its design are explained.

A. Performance Metrics

The performance metrics chosen for the evaluation of black hole attack are packet end-to-end delay, network throughput and network load.

The packet end-to-end delay is the average time in order to traverse the packet inside the network. This includes the time from generating the packet from sender up till the reception of the packet by receiver or destination and expressed in seconds. This includes the overall delay of networks including buffer queues, transmission time and induced delay due to routing activities. Different application needs different packet delay level. Voice and video transmission require lesser delay and show little tolerance to the delay level.

The second parameter is throughput; it is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds. In MANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

The third parameter is network load, it is the total traffic received by the entire network from higher layer of MAC which is accepted and queued for transmission. It indicates the quantity of traffic in entire network. It represents the total data traffic in bits per seconds received by the entire network from higher layer accepted and queued for transmission. It does not include any higher layer data traffic rejected without queuing due to large data packet size.

B. Simulation Tool

The tool used for the simulation study is OPNET 14.5 modeler. OPNET is a network and application based software used for network management and analysis [24]. OPNET models communication devices, various protocols, architecture of different networks and technologies and provide simulation of their performances in virtual environment. OPNET provides various research and development solution which helps in research of analysis and improvement of wireless technologies like WIMAX, Wi Fi, UMTS, analysis and designing of MANET protocols, improving core network technology, providing power management solutions in wireless sensor networks.

In our case we used OPNET for modeling of network nodes, selecting its statistics and then running its simulation to get the result for analysis.

C. Modeling of Network

At first network is created with a blank scenario using startup wizard. Initial topology is selected by creating the empty scenario and network scale is chosen by selecting the network scale. In our case we have selected campus as our network scale. Size of the network scale is specified by selecting the X span and Y span in given units. We have selected 1000 * 1000 meters as our network size. Further technologies are specified which are used in the simulation. We have selected MANET model in the technologies. After this manual configuration various topologies can be generated by dragging objects from the palette of the project editor workspace. After the design of network, nodes are properly configured manually.

D. Collection of Results & Statistics

Two types of statistics are involved in OPNET simulation. Global and object statistics, global statistics is for entire network’s collection of data. And object statistic includes individual node statistics. After the selection of statistics and running the simulation, results are taken and analyzed. In our case we have used global discrete event statistics (DES).

E. Simulation Setup

Figure 6.1 employs the simulation setup of a single scenario comprising of 30 mobile nodes moving at a constant speed of 10 meter per seconds. Total of 12 scenarios have been developed, all of them with mobility of 10 m/s. Number of nodes were varied and simulation time was taken 1000 seconds. Simulation area taken is 1000 x 1000 meters. Packet Inter-Arrival Time (sec) is taken exponential (1) and packet size (bits) is exponential (1024).

The data rates of mobile nodes are 11 Mbps with the default transmitting power of 0.005 watts. Random way point mobility is selected with constant speed of 10 meter/seconds and with pause time of constant 100 seconds. This pause time is taken after data reaches the destination only.

Our goal was to determine the protocol which shows less vulnerability in case of black hole attack. We choose AODV and OLSR routing protocol which are reactive and proactive protocols respectively. In both case AODV and OLSR, malicious node buffer size is lowered to a level which increase packet drop. Furthermore the simulation parameters are given in Table I.

The first simulation was building of normal working MANET with normal behavior of nodes without any type of attack introduced on it (Without Attack) i.e. no malicious node introduced yet. This will lead us to observe and measure the effect of network when there is attack carried on (With Attack) i.e. introduction of malicious nodes.

In case of black hole attack single malicious node is introduced in the whole network. After simulation of the scenario the graphs are analyzed in comparison with normal working protocols of AODV and OLSR (without attack). The malicious node is place in the network between sender and receiver. This malicious node when receive any sort of packets actually discards out all the received data. Now in

simulation we implemented the single malicious node in both AODV and OLSR protocols.

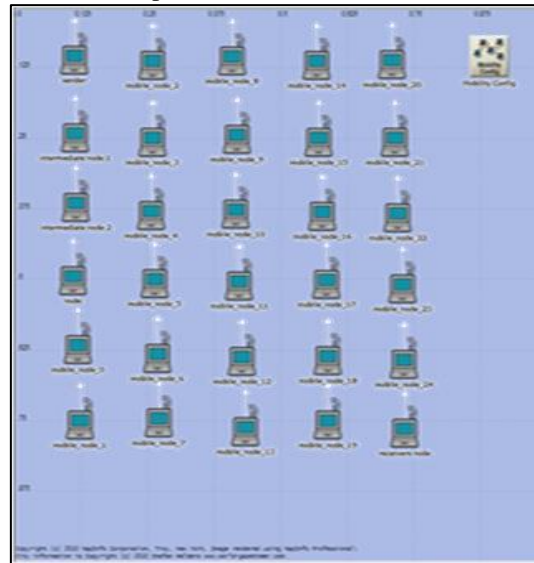


Fig. 6.1: Simulation Environment for 30 nodes

Simulation Parameters	
Examined protocols	AODV and OLSR
Simulation time	1000 seconds
Simulation area (m x m)	1000 x 1000
Number of Nodes	16 and 30
Traffic Type	TCP
Performance Parameter	Throughput, delay, Network Load
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

Table 1:

IX. RESULTS

This chapter focuses on result and its analysis based on the simulation performed in OPNET modeler 14.5. Our simulated results are provided in Figures (7.1-7.12) gives the variation in network nodes while under Black Hole attack. To evaluate the behavior of simulated intrusion based black hole attack, we considered the performance metrics of packet end-to-end delay, throughput and network load. These parameters are already defined in chapter 6 “performance analysis”.

X. CONCLUSIONS & FUTURE WORK

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks with solution finding

technique. Black Hole attack is simulated and its impact on the MANETs is analyzed with three performing matrices i.e. End-to-End delay, Network Load and Throughput. The results obtained from simulation are analyzed deeply in order to draw the final conclusion. Different mitigation plans are studied in detail and we come up with mitigation plan that suits best to eliminate Black Hole attack.

REFERENCES

- [1] C.Jialin, W. Zhiyang, L.Ning, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April, 2010.
- [2] Z.C.Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May, 2010.
- [3] S.Das, A hoc On-Demand Distance Vector (AODV) Routing. July 2003, [Online]. Available: <http://www.faqs.org/rfcs/rfc3561.html>. [Accessed: April. 10, 2010]
- [4] T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-Hoc Networks", Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.
- [5] P.Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626 October, 2003.
- [6] Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July, 2002.
- [7] P.V.Jani, "Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 2002.
- [8] P.Ebinger, "Performance Evaluation of the Impact of Attacks on MANET.
- [9] Hocnetworks", D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Networks", International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.
- [10] U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.
- [11] L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.
- [12] K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks", Proceedings of the 6th annual international conference on Mobile computing and networking, united states, pp. 255-265,
- [13] C. M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.
- [14] V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.
- [15] M.Natue and A.Sethi, "Analysis of Wormhole Intrusion attacks in MANETs", IEEE Military Communications Conference, pp. 1-7, Nov, 2008.
- [16] F. R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", Vol. 35, pp. 22-26, Apr, 2002.
- [17] L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks", International Conference on Networking, Systems, Mobile Communications and Learning Technologies, April, 2006.
- [18] W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks", University of Cincinnati, IEEE Communication Magazine, Oct, 2002.
- [19] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.", International Conference on Computational Intelligence and Security, 2009.
- [20] Opnet Technologies, Inc. "Opnet Simulator", [Online]. Available: www.opnet.com,
- [21] H.Nakayama, N.Kato, A.Jamalipour, Y.Nemoto, "Detecting Blackhole Attack on AODV- Mobile Ad-Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol. 5, No.3, pp. 338-346, Nov, 2007.
- [22] S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-Hoc Networks", ACM Southeast Regional Conf. 2004.
- [23] W. Li, Agrawal, D.P., "Routing security in wireless Ad-Hoc networks", Cincinnati Univ., OH, USA; IEEE Communications Magazine, Vol.40, pp.70- 75, ISSN: 0163-6804, Oct. 2002.
- [24] B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks", In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Computer Science, California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, Nov. 2002.
- [25] Creswell, Research Design: Qualitative, Quantitative and Mixed Methods Approach, 2nd Ed, Sage Publications Inc, California, July 2002.
- [26] S.Selvakumar, "Distribute Denail-of-Service (DDoS) Threat in Collaborative Environment – A survey of DoS Attack Tools and Traceback Mechanism" IEEE International Advance Computing Conference (IACC 2009), pp. 1275-1280, March, 2009.
- [27] Zonglin, H.Guangming, Y.Xingmiao, " Spatial Correlation Detection of DDoS attack" International Conference on Communication, Circuits and System (ICCCAS 2009), pp. 304-308, July, 2009.

Biographies

- [28] Avinash Kamal Mishra pursuing M. Tech in Computer Science (Software Engineering) from BBD University Lucknow , Up, India, my area of research is MANET

[29] Hina Rabbani working as an Assistant Professor in Computer & Engineering Department BBD University Lucknow, Up, India, Her area of research is Network Security.

