International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 4, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Simulation & Analysis of Mobile Ad Hoc Network Statistics at Different Attack Conditions

Gajendra Singh Chandel
Department of Information Technology
Sri Satya Sai Institute Of Science & Technology
Sehore, Bhopal (M.P.), India

Priyanka Murotia
Department of Information Technology
Sri Satya Sai Institute Of Science & Technology
Sehore, Bhopal (M.P.), India

Abstract **– this paper presents an analysis of MANET statistics under different attack conditions the motive of this work is to predict the network condition by its statistics. The analysis is performed by modeling and simulating the different attacks of MANET on network simulator tool. In this paper seven different attacks are simulated & simulation statistics of ten different parameters are taken for analysis the detail of parameters are given in second section of the paper. Finally the simulation results show that statistical behavior can be used for attack detection on MANET.**

Keywords **– MANET, Network Attacks, Network Modeling, Network Simulation**.

I. INTRODUCTION

A MANET is referred to as a network without infrastructure because the mobile nodes in the network dynamically set up temporary paths among themselves to transmit packets. In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. Nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages [1]. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the destination host. Every node functions as a router. The success of communication highly depends on other nodes' cooperation. At agiven time, the system can be viewed as a random graph due to the movement of the nodes, their transmitter/receiver coverage patterns, the transmission power levels, and the co-channel interference levels. The network topology may change with time as the nodes move or adjust their transmission and reception parameters. Possible applications of MANET include: soldiers relaying information for situational awareness on the battlefield, business associates sharing information during a meeting, attendees using laptop computers to participate in an interactive conference, and emergency disaster relief personnel coordinating efforts after a fire, hurricane or earthquake. Other possible applications [1] include personal area and home networking, location-based services, and sensor networks. Security is an essential service for wired and wireless network communications. The success of MANET strongly depends on whether its security can be trusted. However, the characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation. There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV [2] [3]. More sophisticated and subtle routing attacks have been identified in recent

Published papers, such as the black-hole (or sinkhole) [4], Byzantine [5], and wormhole [6] [7] attacks [8].

Table I
Security Attacks Classification

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Jamming, spoofing, modification, replaying, DoS.

Currently routing security is one of the hottest research areas in MANET.

II. RELATED WORK

The following list of papers shows the relative work carried out for different types of attacks in MANETS and possible solutions given.

1) Network layer attacks and defense mechanisms in manets- A survey: In this work a study that will through light on such attacks in MANETS is presented. The work also focuses on different security aspects of network layer and discusses the effect of the attacks in detail through as survey of approaches used for security purpose [15].

2) Wormhole attacks detection in wireless ad hoc networks using a statistical analysis approach [16].

3) Security aspects in manet technical review with security solution: Mobile Ad hoc networks (MANETs) are a new paradigm of wireless network, offering unrestricted mobility without any underlying infrastructure such as base station or mobile switching centers. Basically ad hoc network is a collection of nodes communicating with each other by forming a multi-hop network. In a mobile ad hoc network, it is much more vulnerable to attacks than a wired network due to its limited physical security, dynamically changing network topology, energy constrained operations and lack of centralized administration. Since all the nodes in the network collaborate to forward the data, the wireless channel is

prone to active and passive attacks by malicious nodes, such as Denial of Service (DoS), eavesdropping, spoofing, etc. The intent of this work is to investigate the security goal, security challenges and different types of active and passive attacks on MANETs [17].

4) A highly secured approach against attacks in manet: in this work the implementation of identification and prevention of malicious node launching packet dropping and message tampering attacks [18].

5) Study of different attacks on multicast mobile ad hoc network: in this work simulation based study, the impact of different types of attacks in mobile ad hoc networks. consider the most common type of attacks namely black hole attack and wormhole attack study how these attacks affect the performance metrics of a multicast session such as packet delivery ratio, packet latency and packet-consumed energy[19].

6) a study on wormhole attack in manet.:in this work analyzed the performance of manet under wormhole attack using qos parameter are throughput, delay, node density, packet delivery ratio, power consumption study focus on how qos is affected under wormhole attack in a network[20].

7) Performance analysis of manet before and after black hole attack: in this work simulated manets with and without black hole to study the effects of black hole attack on network performance. Because of black hole attack the average packet drop increased from 0.25% to 90.69%.[21].

8) attacks analysis in mobile ad hoc networks: modeling and simulation: in this work present survey of various attack, and simulation & analysis of attack(only black hole, selfish, flooding) in output variation(in no. of packet send or received),energy consumption[22].

9) Detection and accusation of packet forwarding **misbehavior** in mobile ad-hoc networks using flow of conservation mechanism and done with protocol less implementation [23].

10) A reliable and secure framework for detection and isolation of malicious nodes in manet: this security framework involves detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and prevention data packets by using dispersion techniques [24].

The most of the related study covers only few network layer attacks like black hole, wormhole or as a whole to identify the malicious nodes. In the proposed secured approach, we are simulated 7 types of attacks and then statistical analysis on ten different parameters; finally the simulation results show that statistical behavior can be used for attack detection using svm on manet. in this paper presented only simulation& analysis work.

III. TYPES OF ATTACK IN MANET

This section describes the attacks used for analysis in this paper.

A. Black hole Attack:

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 [9]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [10]. The method how malicious node fits in the data routes varies. Fig. 1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node.

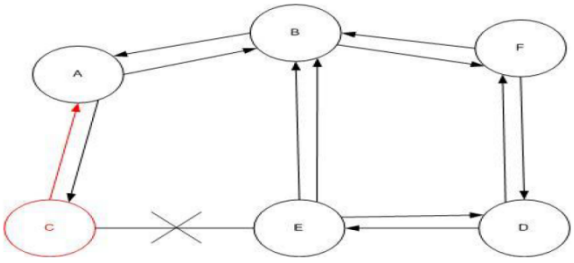

Fig.1. Black hole Attack

In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

B. Wormhole Attack:

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. The fig.2 (bellow) shows the two attackers placed themselves in a strong strategic location in the network.

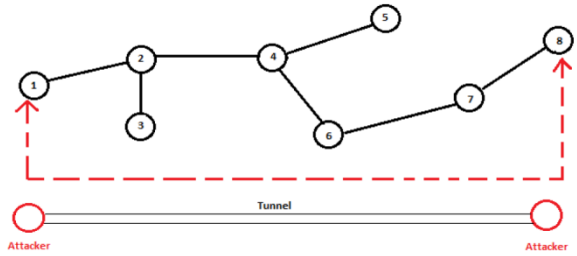

Fig.2. Wormhole Attack

In wormhole attack, 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 as shown in the Fig. 2 (Above). They advertise their path letting the other nodes in the network to know

they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network [11].When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such position the attack is known as out of band wormhole [12]. The other type of wormhole attack is known as in band wormhole attack [12]. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

C. Selfish Attack:

In MANETs the nodes perform collaboratively in order to forward packets from one node to another node. When a node refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disruption [13]. The selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes. The concern of the node is only to save and preserves it resources while the network and traffic disruption is the side effect of this behavior. The node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network. The selfish node can sometime drop the packets. When the selfish node see that the packets need lot of resources, the selfish node is no longer interested in the packets it just simply drop the packets and do not forward it in the network.

D. Sleep Attack:

One of the most interesting attack in MANETs, where the attacker tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep. This attack is known as sleep Deprivation torture attack [14]. The nodes operating in MANETs have limited resources i.e. battery life, the node remain active for transmitting packets during the communication. When the communication cease these nodes go back to sleep mode in order to preserve their resources. The attacker exploit this point of the nodes by making it busy, keeping it awake so as to waste all its energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily walk into the network and exploit rest of the network.

E. Flooding Attack:

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding [13]. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

F. Reply Attack:

This consists in propagating the old routing messages, which do not reflect current topology, in the network to affect routes. To prevent this attack type the mechanism of Sequence Number was proposed and they make it possible for distinction between the old and the new transmitted packets.

IV. Modeling, Simulation & Analysis

After gathering the required details of all types of attack mention in previous section each type of attack is simulated in OPNET network simulator with following simulation parameters.

Table II
Simulation Parameters

Parameter Name	Value
Number of Nodes	20
Simulation Time	60 minutes
Area	1x1 Km.
Node Speed	10 Km/h
Packet Size	1024 bits
Routing	AODV
Transmitter Power	5 mW
Antenna Type	Omnidirectional

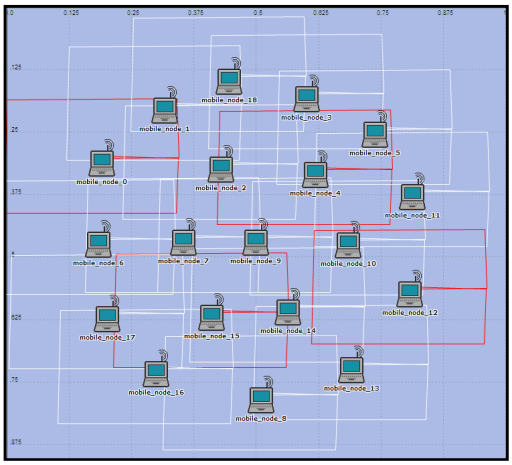

Fig.3. Snap shot of the simulated network.

A. Parameters Description Chosen For Statistical Analysis**.**

*1) Number of Hops per Route***:**

This statistic represents the number of hops in each route to every destination in the route table of all nodes in the network.

2) Route Discovery Time:

The time to discover a route to a specific destination is the time when a route request was sent out to discover a route to that destination until the time a route reply is received with a route to that destination. This statistic represents the time to discover a route to a specific destination by all nodes in the network.

3) Routing Traffic Received:

Amount of routing traffic received in packets/sec in the entire network.

4) Routing Traffic Sent:

Amount of routing traffic sent in packets/sec in the entire network.

5) Total Cached Reply Sent:

When a node receives a route request and is not the target of the route request, it looks up its route table to determine if it has any route to the target of the route request. If so, the node sends back a "Cached Route Reply" and does not re-broadcast the request packet. This statistic represents the total number of cached route replies sent by all nodes in the network.

6) Total Packet Dropped:

When no route is found to the destination, the node drops the packets queued to the destination.

7) Total Replies Sent From Destination:

Once the destination node receives a route request, it sends a route reply to the source of the request. This statistic represents the total number of route reply packets sent from all nodes in the network if they are destinations of route requests. This statistic represents the total number of application packets discarded by all nodes in the network.

8) Total Route Error Sent:

A node may send Hello messages to its neighbor to confirm next hop reachability. If next hop reachability cannot be confirmed, the node sends back a route error message to all nodes that use that next hop to reach various destinations. This statistic represents the total number of route error packets sent by all nodes in the network.

9) Total Route Replies Sent:

A node would send back a route reply to the source of the request; if a) It was the destination of the request b) It had a route to the destination in its route table.

This statistic represents the total number of route reply packets sent by all nodes in the network (both cached route replies and route replies if it's a destination).

10) Total Route Requests Sent:

This statistic represents the total number of route request packets sent by all nodes in the network during route discovery.

After simulating the network with the specified parameters shown in table 2 following results are collected for all seven characteristics parameter.

Color representation used for different types of Attack.

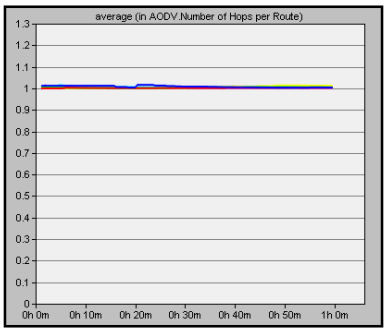

Fig.4. plot for variation in average number of hops per route.

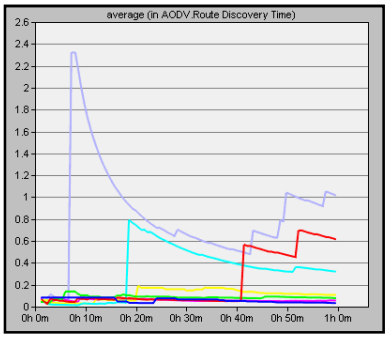

Fig.5. plot for variation in Route Discovery time.

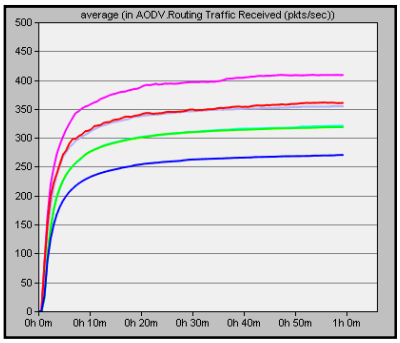

Fig.6. plot for variation in Routing Traffic Received (Packets/Seconds).

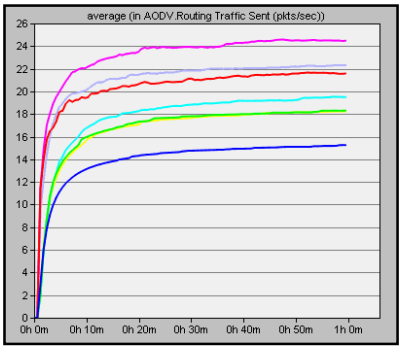

Fig.7. plot for variation in Routing Traffic Sent (Packets/Seconds)

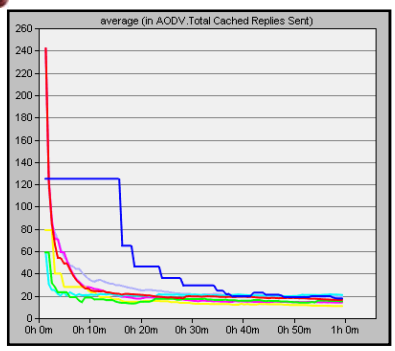

Fig.8. plot for variation in total Cached Reply Sent.

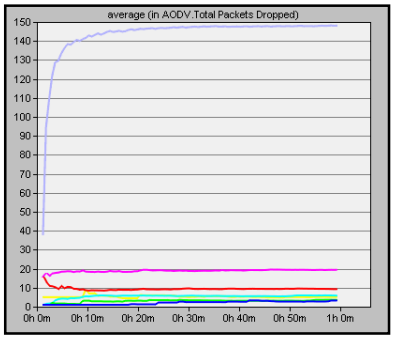

Fig.9. plot for variation in Total Packet Dropped.

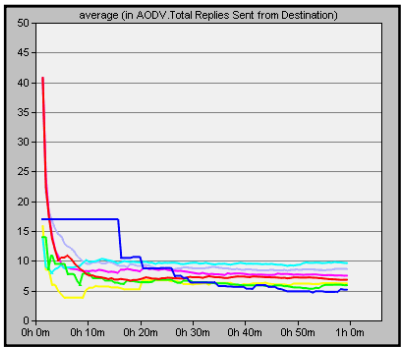

Fig.10 plot for variation in Total Replies Sent from Destination.

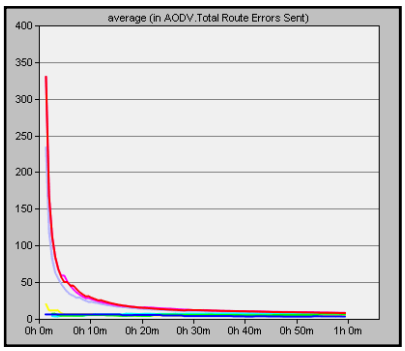

Fig.11. plot for variation in Total Route Errors Sent.

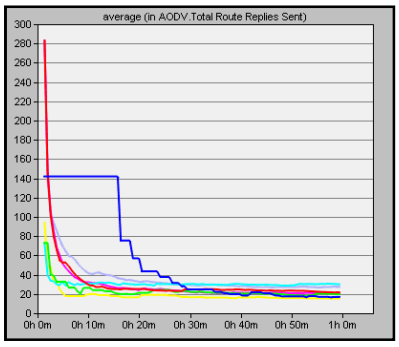

Fig.12. plot for variation in Total Route Replies Sent.

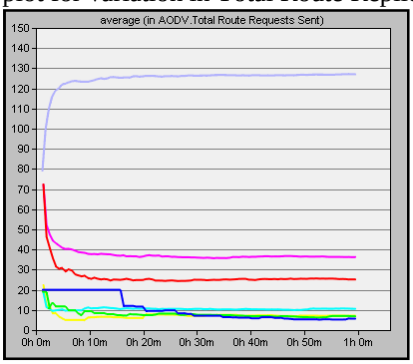

Fig.13. plot for variation in Total Route Requests Sent.

B. Simulation Results from This Part of Algorithm

TABLE III

COLLECTED STATISTICS OF DIFFERENT PARAMETERS FOR WORMHOLE ATTACK

	1	2	3	4	5	6	7	8	9	10
5	1	.1	262	18.1	50	129	13	40	60	120
10	1	1.8	305	20	32	140	9.9	21	41	122
15	1	1.2	325	20.9	28	142	10	18	39	123
20	1	.8	339	21.2	23	143	9.6	17	35	123
25	1	.7	341	21.8	22	144	9	17	34	124
30	1	.67	343	21.9	21	144	9.2	16	30	125
35	1	.61	344	22	21	145	9.3	15	31	126
40	1	.5	348	22	20	146	9.5	14	30	126
45	1	.64	350	22	20	147	9.5	13	30	127
50	1	.79	355	22.1	20	147	9.5	12	30	128
55	1	.97	356	22.1	20	148	9.6	10	31	129
60	1	1.1	358	22.2	20	149	9.6	9	31	129

The table III shows the network statistics for the worm-hole attack. In the table each row shows the collected parameters after certain time of simulation (like 5, 10 and 15 minutes etc.) like above table we simulated the network for Black-hole, selfish, sleep, flooding, and replay attacks & for normal condition.

V. CONCLUSION

The above simulation results shows that the selected parameters shows the sufficient deviation at different attack conditions like Total Route Requests Sent varies from 5 to 35, Routing Traffic Sent (Packets/Seconds) varies from 15 to 24, Route Discovery time from 0.1 seconds to 1 seconds, Total Replies Sent from Destination varies from 5 to 10 & Total Packet Dropped varies from 5 to 150 depending upon the type of attack applied to network. Hence these parameters can be taken as the

characteristics parameter which reflects the network condition and can be used to classify the attacks.

REFERENCES

[1] C. Perkins "Ad Hoc Networks", Addison-Wesley, 2001.
[2] M. Zapata "Secure Ad Hoc On-Demand Distance Vector (SAODV)" Internet draft, draft-guerrero-manet-saodv-01.txt 2002.
[3] Y. Hu, A. Perrig, and D. Johnson "Ariadne : A Secure On-Demand Routing for Ad Hoc Networks" Proc. of MobiCom 2002, Atlanta, 2002.
[4] Y. Hu and A. Perrig "A Survey of Secure Wireless Ad Hoc Routing" IEEE Security & Privacy, pp. 28-39, 2004.
[5] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens "An On-demand Secure Routing Protocol Resilient to Byzantine Failures" Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.
[6] Y. Hu, A. Perrig, and D. Johnson "Packet Leashes: A Defense Against Worm-hole Attacks in Wireless Ad Hoc Networks" Proc. of IEEE INFORCOM, 2002.
[7] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer "A Secure Routing Protocol for Ad Hoc Networks" Proc. of IEEE International Confer-ence on Network Protocols (ICNP), pp. 78-87, 2002.
[8] Xiao, X. Shen, and D.-Z. Du (Eds.) "Wireless/Mobile Network Security" 2006 Springer.
[9] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.
[10] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006.
[11] N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-Hoc Network".
[12] V.Mahajan, M.Natue and A.Sethi, "Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.
[13] M.T.Refaei, 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.
[14] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.
[15] G.S. Mamatha, dr. S.C. Sharma" network layer attacks and defense mechanisms in manets- A survey" in international journal of computer applications (0975 – 8887) volume 9– no.9, November 2010.
[16] N. Song, L. Qian, X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach", Parallel and Distributed Processing Symposium, Proceedings, 19th IEEE International, 2005.
[17] Monika, Mukesh Kumar, Rahul Rishi "Security Aspects In Mobile Ad Hoc Network (Manets): Technical Review "In international Journal Of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010.
[18] G.S. Mamatha AND DR. S. C. Sharma " A Highly Secured Approach Against Attacks In Manet- IN INTERNATIONAL JOURNAL OF COMPUTER THEORY AND ENGINEERING, VOL. 2, No. 5, October, 2010.
[19] N.Shanthi, DR.Lganesan AND DR.K.Ramar" Study Of Different Attacks On Multicast mobile Ad Hoc Network IN JOURNAL OF THEORETICAL AND APPLIED INFORMATION TECHNOLOGY.
[20] Reshmi Maulik and Nabendu Chaki" A Study on Wormhole Attacks in MANET" in International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011)
[21] Ms. Heena Bhalla" PERFORMANCE ANALYSIS OF MANET BEFORE AND AFTER BLACK HOLE ATTACK"in Int.J.Computer Technology & Applications, Vol 3 (1),
[22] Dr. Karim Konate, GAYE Abdourahime" Attacks Analysis in mobile ad hoc networks" 2011 Second International Conference on Intelligent Systems, Modeling and Simulation.
[23] Oscar F. Gonzalez, God win Ansa, Michael Howarth, and George Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, vol-2, 2008, pp.1.
[24] S. Dhanalakshmi, Dr. M. Rajaram, "A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET", IJCSNS International Journal of Computer Science and Network Security, vol-8. No.10, October, 2008.

AUTHOR'S PROFILE

Prof. Gajendra Singh Chandel
Head of Department of SSSIST, Sehore, India. He did his M.Tech.(CS) from LNCT, Bhopal in year 2007.

Priyanka Murotia
M.Tech. (IT) final year student of SSSIST, Sehore. He did his B.E. (CS) from GRKIST, JBL, India in year 2007.