Black Hole Detection in MANET using AODV Routing Protocol

Govind Sharma, Manish Gupta

Abstract— ***Mobile Ad-hoc network (MANET) has become an individual part for communication for mobile device. Therefore, interest in research of Mobile Ad-hoc network has been growing since last few years. Due to the open medium, dynamic network topology, autonomous terminal, lack of centralized monitoring and lack of management point Mobile Ad-hoc network are highly vulnerable to security attacks compared to wired network or infrastructure-based wireless network. In this paper, we analyze the black hole attack. In this attack, a malicious node falsely advertise shortest path to the destination node. The intension of malicious node could be to intercept all data packets being sent to the destination node concerned. We proposed our approach to detect the black hole attack in Mobile Ad-hoc network. This approach is based on the AODV (ad-hoc on demand distance vector) routing algorithm. In this paper we are enhancing the secured AODV routing algorithm. Here we are making more secure AODV routing algorithm and using promiscuous mode of the node in promiscuous mode node can learn about the neighbouring routes traversed by data packets if operated in the promiscuous mode.***

***Keywords*— Secured Routing, AODV, Ad-hoc network, Black Hole Attack, Malicious node,MANET.**

I. INTRODUCTION

A mobile ad-hoc network [1][2], **is** a self organized network. Mobile ad-hoc network consists of a site of wireless mobile nodes that are capable of communicating with each other with no use of any centralized administration. Communication in mobile ad-hoc network done via multi-hop path. If two mobile nodes are inside each other's transmission range. They can communicate directly. Otherwise, the nodes in between forward the packet for them. In such a case, every mobile node has to function as a router to forward the packet. Routing in mobile ad-hoc network faces additional problem and challenges when compared to routing in traditional wired network. Other Some unique and attractive features of mobile ad-hoc network as such no fixed infrastructure, automatic self configuration and maintenance, quick deployment, no centralized administration. Each node in mobile ad-hoc network is free to move independently. Due to the flexibility of mobile ad-hoc network node can join and leave a network easily. But this flexibility of mobile nodes result in a dynamic topology that makes it very hard in developing secure ad-hoc routing protocol.

Since the nodes are mobile, the network topology may change rapidly and unpredictably and connectivity among the terminal may vary with the time. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming own network on the fly. The link capacity fluctuates in the mobile ad-hoc network. The nature of high bit error rates of wireless connection might be more profound in a MANET. Since there is no background network for the central control of the network operation, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves.

Many routing protocols [16] for mobile ad hoc networks have been proposed. Routing in mobile ad-hoc network faced other problem and challenges compared to routing additional wired network. There are several well-known protocols in the literature that have been particularly developed to handle with the limitations imposed by ad hoc networking environments. The problem of routing in such environments is motivated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth, and high error rates [24].

Most of the existing routing protocols follow two different design approaches to deal with the inherent characteristics of ad hoc networks: the table-driven and the source-initiated on-demand approaches [3].

Table-driven: Table driven routing protocols fundamentally use proactive schemes. They attempt to maintain reliable up-to-date routing information from every node to every other node in the network. These protocols need each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a reliable network view. Destination-Sequenced Distance-Vector (DSDV) protocol [4] and the Optimized Link State Routing (OLSR) protocol [5] are examples of this category of protocols.

Source-initiated on-demand: A different approach from table driven routing is source-initiated on-demand routing. This kind of routing creates routes only while desired by the source node. When a node requires a route toward destination, it initiates a route finding process inside the network. A route is acquired by the initiation of a *route discovery* function by the source node. The data packets transmitted as a route finding is in process are buffered and are sent when the path is established. An established route is maintained as long as it is required during a *route maintenance* procedure. The Ad hoc On-demand Distance Vector (AODV) routing protocol [1] and the Dynamic Source Routing protocol [6] are examples of this category of protocols.

Manuscript received December 21, 2011
Govind sharma, Email: bobby_mits@yahoo.com
Manish Gupta, Email: manishgupta.2007@gmail.com

II. ROUTING SECURITY IN MANETS

Security always implies the identification of potential attacks, threats and vulnerabilities of a certain system. Janne Lundberg [7] discussed special types of attacks that can simply be performed against a MANET. Attacks can be classified into *passive* and *active attacks*. A passive attack does not interrupt the operation of a routing protocol, but only attempts to find out valuable information by listening to routing traffic, which makes it very difficult to detect. An active attack is an attempt to modify data, gain authentication, or acquire authorization by inserting fake packets into the data stream or modifying packets transition in the network. Active attack can be divided into external attacks and internal attacks. .In *external attack*
nodes do not belong to the network. An *internal attack* is one from compromised or hijacked nodes that belong into the network.

Based on this threat analysis and the recognized capabilities of the potential attackers, we will now discuss several specific attacks that can target the function of a routing protocol in an ad hoc network.

Black Hole: A black hole [9] is a type of denial of service attack where the intension of the malicious node could be to hinder the path finding process or to intercept all data packets being sent to the destination node.

Location Disclosure: Location disclosure [8] is an attack that targets the confidentiality requirements of an ad hoc network. Through the utilize of traffic analysis techniques, or with simpler probing and monitoring approaches, an attacker is able to find out the location of a node, or even the structure of the whole network.

Replay: An attacker in replay attack [1] an attacker injects into the network routing traffic that has been captured previously. This attack generally targets the newness of routes, but can also be used to undermine badly designed security solutions.

Energy consummation: Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmit only when absolutely necessary. An attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node [1].

Blackmail: This attack is relevant against routing protocols that use mechanisms for the recognition of malicious nodes and transmit messages that attempt to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legal nodes from the network [25].

III. AODV ROUTING PROTOCOL AND BLACK HOLE ATTACK

Ad hoc on-demand distance vector (AODV) routing protocol[1][21], uses on-demand approach for finding routes, that is, a route is established only while it is required by a source node for transmitting data packets. It employs destination sequence number to recognize the most recent path. In AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the RREQ packet in the network when a route is not available for the desired destination. It may obtain multiple routes to different destinations from a single RREQ. AODV routing uses a destination sequence number to determine up-to-date path to the destination. Destination sequence number indicates the newness of the route that is accepted by source. When an intermediate node receives a RREQ, it either forwards it or prepares a RREP if it has a valid route to the destination. All intermediate nodes having valid route to the destination, or the destination node itself, are permitted to send RREP to the source. RREP is a unicast message back along the saved path to the source node or it re-broadcast the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has a fresh route to the destination node is received by the source node. As the RREP is propagated back toward the source, all intermediate nodes set up forward route entry in their tables. The route maintenance process utilizes link-layer notifications, which are intercepted by nodes neighbouring the one that caused the error. These nodes produce and forward route error (RERR) messages to their neighbours that have been using routes that contain the broken link. Following the reception of a RERR message a node initiates a route discovery to replace the disastrous paths.

AODV is a collaborative protocol [10] and allow nodes to distribute the information they hold about other nodes. RREQ messages need not necessarily reach the destination node during the route discovery process. If an intermediate node already knows a route toward the destination, it does not forward the RREQ any further and generates a RREP message. This enables quicker replies and limits the flooding of RREQs when flooding is not required.

Route discovery is vulnerable in AODV, which an adversary can exploit to perform a black hole attack on mobile ad-hoc network. In this attack, a malicious node falsely advertised excellent path (e.g., shortest path or more stable path) to the destination node during the path finding process. The intension of the malicious node could be to hamper the path-finding process or to intercept all data packet being sent to the destination node concerned.

IV. AODV SUFFERS WITH BLACK HOLE ATTACK

A black hole [1][9], is a type of denial of service attack where the intension of the malicious node could be to hinder the path finding process or to intercept all data packets being sent to the destination node. In this attack the malicious node listen to a route request packet in the network, and respond with claim of having an extremely short route to the destination node, even if it does not have any such route. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

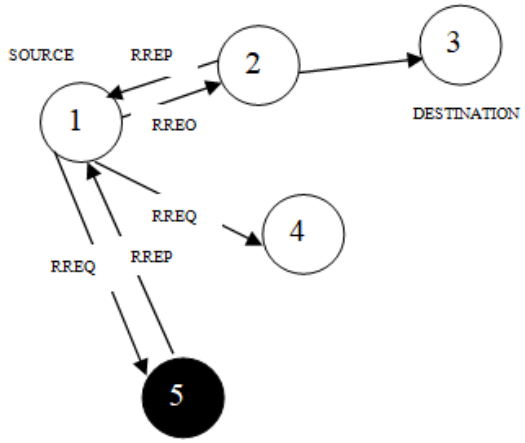

Figure 1 Routing discovery in AODV with black hole attack

In the following Figure 1 source node (node1) broadcasts a route request packet RREQ to its neighbours to discover a route to the destination node3. We assume that routing table of node2 have a route to the destination node3 and node5 is the malicious node in the network, when the node1 sends a RREQ packet to its neighbour node2, node4 and node5. Malicious node5 will not check its own routing table, and directly sends a fake RREP to node1, so the malicious RREP reaches fastest to the node1 as compare to the other nodes in the network. At this time node1 accept the short route from the malicious node5 and rejects the other RREP packets and sends application layer data toward destination node along the opposite direction route of the malicious node RREP. Source node1 believe that the data has been sent to destination node3, in fact, data has been discarded by the malicious node5. A malicious node (performing a black hole attack) drops all data packets rather than forwarding them to the destination.

V. LITERATURE SURVEY

Various technique have proposed in MANET to detect and prevent black hole attack according to the approach by Songbai Lu et al. [9], proposed SAODV routing , SAODV's basic working principal is very similar to AODV routing. This SAODV directly validate the destination node by node by using the exchange of random number in routing discovery phase, when the source node receive RREP it immediately sends the SRREQ to the destination node along the opposite direction of RREP received. The content of each SRREQ contain a random number (name as x) generated by the source node. When destination node receives SRREQ, destination node will send SRREP containing random number y to s. The disadvantage of this approach is that, in this approach s needs continue to wait, until at least two SRREP, whose content contains a same random number, come from different paths. In paper [14], proposed technique intrusion detection using anomaly detection (IDAD) use host base scheme. Network based intrusion detection schema cannot be engaged to MANET where there is no central device that monitor traffic flow, network based intrusion detection system lying on data centric point of a network such as router and switches but host based intrusion detection system are installed on hosts so that they can oversee the activities of a host and users on the hosts. IDAD assumes every activity of a user or a system can be recognized from normal activities. IDAD needs to be provided with a pre collected set of anomaly activities, called audit data. IDAD system capable to compare every activity of a host with the audit data, if any activity of a host match the activity listed in the audit data, the IDAD system separate the particular node from the network. The drawback of this technique is that, here needs the extra memory to make IDAD system. In paper [11], presents the extension of association based routing which is to be applied over the DSR protocol to enhance the security. In this approach every node in the network a trust value is store that represents the value of the trustiness to every of its neighbour nodes. This trust value will be adjusted based on the experience that the node has with its neighbour. In proposed scheme organize the association among the node and their neighbour node keen on three category these category are unknown, known and companion based on their trust value among the nodes. This trust value evaluate by using the different parameter, however in the real network it is very complex to set an appropriate value for the trust level. In paper [20], introduce the use of DRI (Routing Information) to keep track of past routing information among mobile nodes in the network and cross checking of RREP message from intermediate node by source node. The main disadvantage of this technique is that mobile node has to maintain an extra database of precedent routing knowledge in addition to routine work of maintaining their routing table. In paper [17], every node crosses check with its next hop node on the route to the destination on receiving or overhearing a RREP packet. If the next hop node does not have a link to the node that sent the RREP, then the node sent the RREP consider as malicious node. The drawback of this approach is that, this approach increases the delay in the network. In paper [12], used three components network cluster formation, feature extraction and anomaly detection, in this paper used cooperative intrusion detection methodology there is only one node within each cluster performing the function of anomaly detection. In paper [19], AODV routing protocol is modified in order to adapt the trust based communication. In this paper trust based routing protocol is equally concentrates both in node trust and route trust, Ad hoc network also defined as trusted network. Continuous evaluation of node's performance and collection of neighbour node's opinion value about the node are used to calculate the trust relationship of this node with other nodes. In paper [21], discussed the survey of methods of detecting the black hole attack. CONFIDANT protocol works as an expansion to reactive source routing protocols like DSR [23]. The fundamental idea of the protocol is that nodes that does not forward packets as they are supposed to, will be recognized and expelled by the other nodes. Thereby, a disadvantage is, if a node is found to be intolerable then all the routes which consists of this node will be deleted.

To defend against the black hole attack and to overcome the disadvantage listed above, we proposed a new black hole detection method based on the AODV routing protocol o make it more secure routing protocol.

VI. THE PROPOSED SCHEME FOR BLACK HOLE DETECTION

This section presents the secure AODV routing protocol to enhance the security of the AODV routing protocol. In the proposed scheme we are using the promiscuous mode of the node.

In this mode nodes can also learn about the neighboring routes traversed by the data packets if operated in the promiscuous mode, in other words, promiscuous mode means that if a node A within the range of node B, it can overhear communication to and from B even if those communication do not directly involve A.

Algorithm to detect black hole attack:

EVENT Node "S" have Data for node "D"

Notations:

RREQ: Route Request Packet
RREP: Route Reply Packet
S : Source Node
D : Destination Node

```
S  Send RREQ;
                    /* Start to search the Route for
                       Destination */

Initialize_ timer_T_RREQ;
                    /* Timer, for checking Route Reply
                       time out */

set  original_destination_path=false;

flag = true;

while (flag = true)

if [ RREP from original destination ]

then

set original_destination_path = true;
                                    /* flag used to check
                                       that destination is
                                       connected or not */
flag = false;
end if

if [ intermediate_node _RREP ](name as nth node)

then

(n-1)th nodes (name as x) on its promiscuous mode;
                            /* on hop before of nth nodes
can
                               overhear the route of nth node
*/

X send plane packet to D through node n;
                            /* to check the nth node either
                               It is forwarding data or not
*/
     If
          Plane packet is not forwarded through n;
                            /* nth node drops the plane
                               Message */
     then
          X broadcasts the alarm to all other nodes;
                            /* inform other node there is a
                                        malicious node in the network
*/

          Stop the transmission through this path;
                            /* they will not forward the
RREP
                                towards S */
     else
          nth node is a trusty node;
                            /* nth node is not dropped the
                               Packet */

          set original_destination_path = true;
                            /* forward the RREP towards S
*/

          flag=false;

  end if

end if

if [ T_RREQ expire ]

then

 flag = false;

end if

end while

if [ original_destination_path = true ]

then

establish path and send data;
```

In the proposed scheme we are using the promiscuous mode of the node. In this mode nodes can also learn about the neighbouring routes traversed by the data packets if operated in the promiscuous mode, in other words, promiscuous mode means that if a node A within the range of node B, it can overhear communication to and from B even if those communication do not directly involve A. In suggested approach if the source node have data for destination node then source node need to find the route to the destination node. Initially Source node broadcasts the route request packet for search the route to the destination node and initialize timer in route request packet for checking the route reply time out. In AODV routing all intermediate nodes having valid route to the destination, or destination node itself, are allowed to send the route reply to the source node. In above algorithm if the route reply is from the original destination then route is assumed to be safe and end the data through this path. Otherwise, route reply from the any intermediate node (name as nth node), in this case by analysing of APN count field [26] (The number of accumulated path nodes appended to the RREP) in RREP, node that are one hop (name as x) before of this nth node will on its promiscuous mode packet so that they can overhear the route of nth node.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

After that the x will send the plane packet to destination node through node n to check either nth node forwarding the data or not. If the nth node drops the plane packet then x will broadcasts the alarm to all other nodes to inform that there is a malicious node in the network otherwise the nth node is a trusty node.

VII. SIMULATION AND RESULTS

We are using QualNet 5.0.1 simulator [22]. QualNet is a network simulation tool that simulates wireless and wired packet mode communication network. Qualnet provides a comprehensive environment for designing network protocol, creating and visualizing scenarios under user specific condition and analysing their performance.

We are using QualNet 5.0.1 simulator. For our simulations, we make use of CBR (Constant Bit Rate) application, UDP/IP, IEEE 802.11b MAC and physical channel based on statistical propagation model.

The simulated network consists of 40 at random allocated wireless nodes in a 1500 by 1500 square meter flat space. The node radio range is 250- meter power range. Random waypoint mobility model is used for scenarios. The selected pause time is 30s seconds. A traffic generator was developed to simulate constant bit rate (CBR) sources. The maximum segment size is 512 bytes. In our scenario we take 40 nodes.

Table 1 Scenario specification

Parameter	**Value**
Simulation duration	30 sec.
Simulation area	1500 meter×1500 meter
N0. of nodes	40
Maximum segment size	512 bytes
Data rate	2 mbps
Radio range	250 meter
Traffic type	CBR
Mobility	Random way point

Table 2 Simulation results of throughput

S.No.	Node Mobility (mps)	Throughput in AODV without black hole attack (%)	Throughput in AODV with black hole attack (%)	Throughput in proposed algorithm with black hole attack
1	10	95	65	92
2	20	78	42	76
3	30	66	37	63
4	40	57	19	52

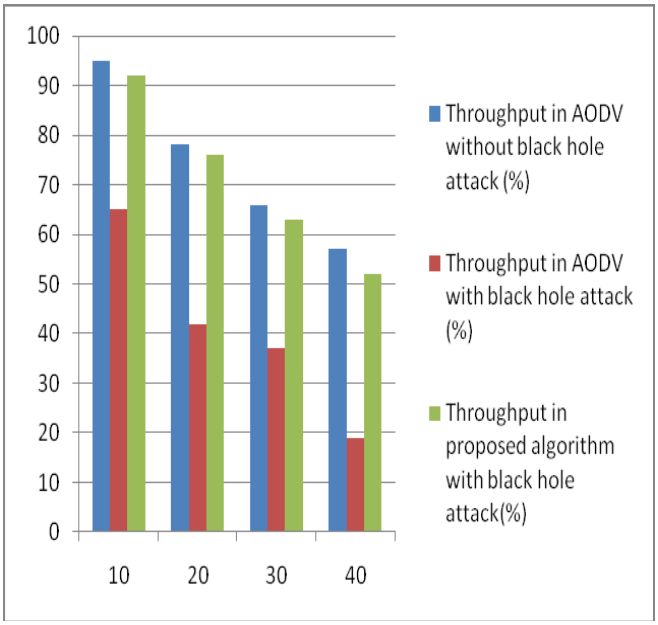

Figure 2 Impact of black hole on network Throughput and throughput in proposed algorithm under black hole attack

In Figure 2 representing the impact of black hole attack on network throughput. The throughput of network is decreased due to the impact of black hole but the proposed algorithm giving the good throughput with black hole attack.

Table 3 Simulation result of End-to-End delay

S.No.	Node Mobility (mps)	End-to-End delay in AODV without black hole attack (%)	End-to-End delay in AODV with black hole attack (%)	End-to-End delay in proposed algorithm with black hole attack (%)
1.	10	.080	.055	.122

2.	20	.131	.112	.147
3.	30	.129	.123	.176
4.	40	.187	.101	.204

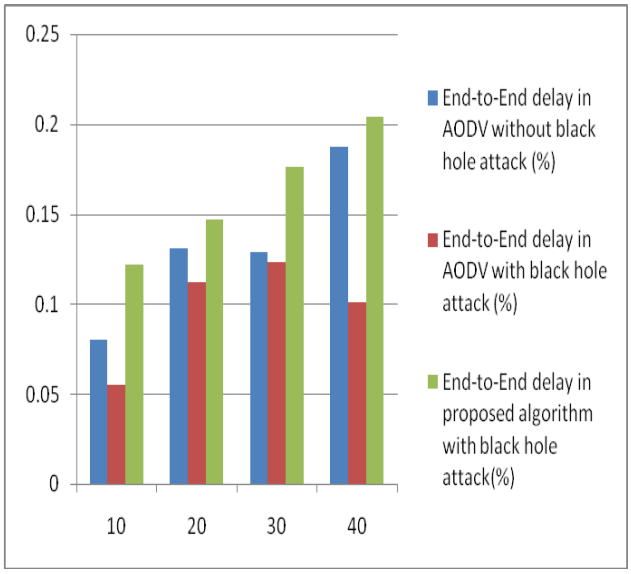

Figure 3 Impact of black hole on network End-to-End delay and End-to-End delay in proposed algorithm under black hole attack

From the figure 3 it can be observed that, there is slight increase in the average end-to-end delay without the effect of black hole, as compared to the effect of black hole attack, This is due to the immediate reply from the malicious node i.e. the nature of malicious node here is it would not check its routing table.

VIII. CONCLUSION

In this paper, we have analysed and describe the condition to detect the single black hole in the network. We have used AODV routing protocol and we have make it more secure routing protocol and propose a feasible solution to detect the black hole attack. Security of our approach is better than AODV's security. In our approach, we are not using extra database for detection of malicious activity. Here we are saving memory requirement for detection of black hole attack.

REFERENCE

1. C. Siva Ram Murthy and B.S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols," Prentice Hall (2004).
2. Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE Communications Surveys & Tutorials, Vol 10, No. 4 pp. 78-93 (2008).
3. D. P. Agrawal and Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*, Brooks/Cole Publishing, Aug. 2002.
4. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector (DSDV) for Mobile Computers,"*Proc. ACM Conf. Commun. Architectures and Protocols (SIGCOMM'94)*, London, UK, Aug. 1994, pp. 234–44.
5. T. Clausen *et al.*, "The Optimized Link State Routing Protocol: Evaluation Through Experiments and Simulation," *Proc. 4th Int'l. Symp. Wireless Pers. Multimedia Commun.*, Aalborg, Denmark,Sept. 2001.
6. D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks,"*Ad Hoc Net.*, C. E. Perkins, ed., Addison-Wesley, 2001, pp. 139–72.
7. J. Lundberg, "Routing Security in Ad Hoc Networks,"Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html
8. J.-F. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems," *Proc. Wksp. Design Issues in Anonymity and Unobservability*, Berkeley, CA, July 2000, pp. 7–26.
9. Songbai Lu, Longxuan Li, Kwon-Yan Lam and Lingvan Jia "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," International Conference on Computational Intelligence and Security, pp 421-425 (2009).
10. Devid Cerri, Alessandro Ghioni, CEFRIEL-Politecnico di Milano "Securing AODV: The A-SAODV secure Routing Prototype," IEEE Communication Magzine, pp 120-125 (2008).
11. N. Bhalaji, A. Shanmugam, "Association between nodes to combat black hole attack in DSR based MANET," Wireless and Optical communication Networks, pp 1-5 (2009).
12. M. Sayee Kumar, S. Selvarajan, S. Balu, "ANODR based anomaly detection for black hole and route disrupt attacks," International Conference on Computing, Communication and Networking , pp 1-5 (2008).
13. Nidhi Sharma, Sanjeev Rana and R.M. Sharma, "Provisioning of Quality of Se Service in MANETs Performance Analysis & Comparison (AODV AND DSR), " International Conference on Computer Engineering and Technology, pp 243-248 (2010).
14. Yibeltal Fantahun Alem and Zhao Cheng Xuan, "Preventing Black Hole Attack in Mobile Ad-Hoc Networks Using Anomaly Detection," International Conference on Future Computer and Communication, pp 672-676 (2010).
15. Martuja Ahmad, Rima Pal and Md. Abu Naser Bikas, "PIDS: A packet based approach to network intrusion detection and prevention," International Conference on Information Management and Engineering, pp 124-127 (2009).
16. Patroklos G. Argyroudis and Donal O'Mahony, "Secure Routing for Mobile Ad-hoc Network," IEEE Communication Surveys & Tutorials, pp 2-21 (2005).
17. Hongmei Deng, Wei Li and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Communication Magazine, Vol. 40 pp 70-75 (2002).
18. Satyabrata Chakrabarti and Amitabh Mishra, "QoS Issues in Ad Hoc Wireless Networks," IEEE Communications Magazine, Vol. 39, pp 142-148 (2001).
19. A. Menaka Pushpa, "Trust Based Secure Routing in AODV Routing Protocol," IEEE, (2009).
20. H. Weerasinghe and H. Fu. "Preventing cooperative black hole attacks in mobile ad-hoc networks: simulation, implementation and evaluation," International Journal of Software Engineeringand its Applications. Vol.2, No. 3 pp. 362-367 (2008).
21. A. Raja Mahmood and A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks,", pp. 1-6 (2007).
22. Scalable Network Technologies (SNT). *QualNet*.http://www.qualnet.com/.
23. Sonja Buchegger and Jean-Yves Le Boudec: "Performance analysis of the CONFIDANT protocol" Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing'02. p.p:226 – 236.http://doi.acm.org/10.1145/513800.513828.
24. E. M. Royer and C.-K. Toh, "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks," *IEEE Pers. Commun.*,vol. 2, no. 6, Apr. 1999, pp. 46–55.
25. L. Zhou and Z. J. Haas, "Securing Ad hoc Networks," *IEEE Net. Mag.*, vol. 6, no. 13, Nov./Dec. 1999, pp. 24–30.
26. tools.ietf.org/html/draft-perkins-manet-**aodv**bis-00

AUTHORS PROFILE

Mr. Govind Sharma obtained Master of Technology (M.Tech.) in Computer Science from ABV-Indian Institute of Technology & management, Gwalior in 2011. The area of research is Wireless Network and Soft Computing.

Mr. Manish Gupta obtained Master of Technology (M.Tech.) in Computer Science from ABV-Indian Institute of Technology & management, Gwalior in 2011. The area of research is Soft Computing and Wireless Network.