Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Routing attacks and their Counter Strategies in MANET

Aditi Kumar, Parveen Thakur
CSE/IT, BUEST
India

Abstract*— Mobile Ad-Hoc Network is a collection of wireless nodes forming a temporary network without using any centralized administration thus letting the nodes of MANETs possess unique characteristics of self-organizing and self -configuring. These nodes operate both as communication end points as well as routers, thus making the wireless adhoc network more vulnerable to security attacks than their wired counterpart. Security attacks can be launched towards any layer of the protocol stack. In this paper, we will walk through some of the common attacks on the Network layer such as Blackhole attack, Wormhole attack and the Grayhole attack which fall under the category of Denial-of-Service Attack (DoS) and their countermeasures that can work for different routing protocols.

***Keywords*— MANET, Security, Blackhole Attack, Wormhole Attack, Grayhole Attack, DoS Attack.**

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes (i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer) that are free in moving in and out in the network. As the nodes are not in the communicating range of all other nodes, the nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure [1]. Figure 1 is an image of a Mobile Adhoc Network.

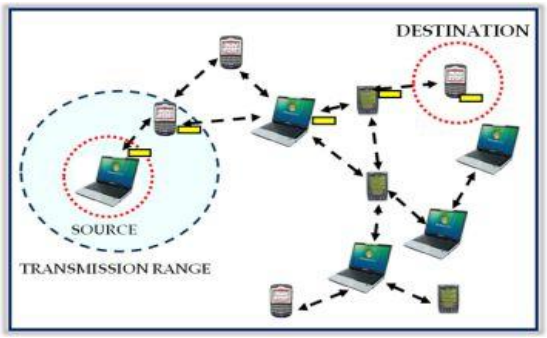

Figure 1: Mobile Adhoc Network

On the other side, the inherent characteristics of MANET leads to some major issues such as routing protocols, power constraints, mobility management, Quality of Service (QoS) and security. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management. Thus in the absence of centralized administration the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the on-going communication [2].

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. In this paper, we have surveyed the various Dos attacks and their counter strategies. The rest of the paper is organized as follows. In Section 2 we introduce the fundamentals of routing and a glimpse of various routing protocols in MANET. Section 3 is a walk through the various security concerns including types of attack with a varied range targeting the various layer of the protocol stack. In Section 4 we give a detail insight on the Dos attacks like Blackhole , Wormhole and the Grayhole attacks along with proposed strategies for prevention and detection of same. Finally in Section 5 we give the conclusion and the future directions.

II. ROUTING IN MANET

Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialized router itself, thus in turn reducing the routing overhead in comparison to that in wired network.

At the same time routing is also a big challenge in MANET, due to mobility of the nodes which may result in change in the route [1]. The primary goal of a routing protocol designed for MANET is of finding an optimal route with minimal overhead and at the same time consuming minimum bandwidth. Various categories that have been identified for classifying of the routing protocols along with their characteristic features are discussed below [1, 3].

A Proactive routing protocol (Table driven)

In this routing scheme every node continuously maintains complete routing information of the network. This is achieved by flooding network periodically with network status information to find out any possible change in network topology. Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment. A new set of routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm.

B Reactive routing protocol (Demand driven)

Every node in this routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route. Rapidly changing wireless network may break active route and cause subsequent route search.

C Hybrid routing protocol

Is a combination of good characteristics of the above 2 stated protocols. Efficiency of hybrid protocols may vary with the number of nodes and the amount of traffic decides the reaction to demand.

The hierarchy of these protocols is shown below in the Figure 2

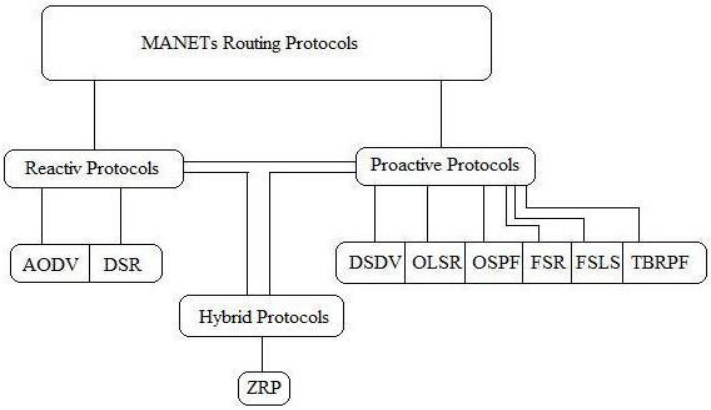

Figure 2: Classification of Routing Protocols

III. SECURITY CONCERNS

Security is an essential component for the widespread use of MANET. The unique characteristic of MANET i.e. dynamic and continuously changing network topology, resource constraints such as limited battery power and bandwidth makes it difficult to use the existing security schemes for the conventional networks directly for MANETs [4]. An attacker by passively or actively attacking on MANET can violate one or the entire security goal such as availability, confidentiality, integrity, authentication, non-repudiation and access control [5]. TABLE-I shows the classification of attacks with their characteristic feature and few examples. Both the type of attacks can be launched on any of the layers of protocol stack. Figure 3 shows various examples of the attacks at different layers.

TABLE-I ROUTING ATTACKS

Type of Attack	Characteristics	Examples
Active Attack	Disturbs network operation by • Modifying or deleting information • Injecting a false message • Impersonating a node Attacker can be internal or external to the network	Modification, impersonation, fabrication, jamming and message replay
Passive Attack	Obtains information without disturbing normal network operation. Difficult to detect.	Traffic analysis, monitoring eavesdropping.

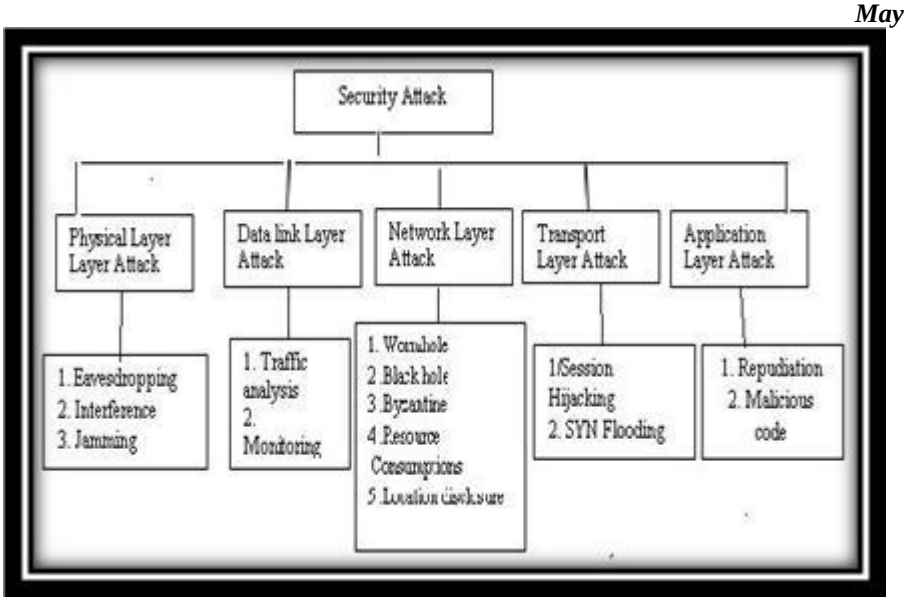

Figure 3: ATTACKS ON DIFFERENT LAYERS OF PROTOCOL ATTACK

In this paper, our prime focus will be on some of the DoS attacks that come under the category of network layer attacks.

IV. DoS ATTACKS

A Denial of Service (DoS) attack is one that attempts to prevent the victim from being able to use all or part of his/her network connection. Denial of service attacks may extend to all layers of the protocol stack. They target service availability or authorized users' access to a service provider. We will discuss Blackhole,Wormhole and Grayhole attacks as well as existing solutions to detect and fight against them.

A Blackhole attack

Black hole attack is one of the kinds of Denial Of Service (DoS) attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [22]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply. The attacker now drops the received messages instead of relaying them as the protocol requires [23].

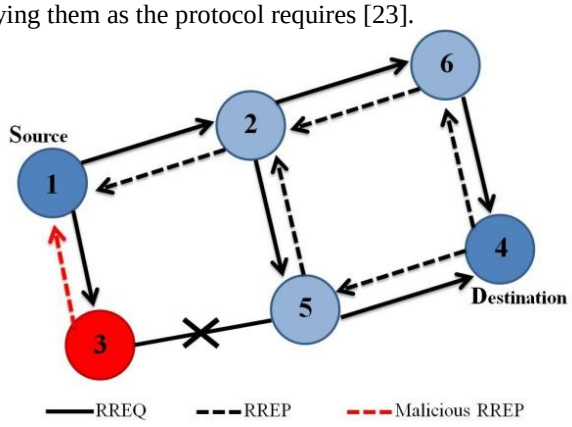

Figure 4: Blackhole attack

1. Operation of Black Hole Attack

In the figure 4, imagine a malicious node "3". When node "1" broadcasts a RREQ packet, nodes "2", and "3" receive it. Node "3", being a malicious node, does not check up with its routing table for the requested route to node "4". Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node "1" receives the RREP from "3" ahead of the RREP from "2". Node "1" assumes that the route through "3" is the shortest route and sends any packet to the destination through it. When the node "1" sends data to "3", it absorbs all the data and thus behaves like a Black hole[24]. In AODV, the sequence number is used to determine the freshness of routing information contained in the message from the originating node. When generating RREP message, a destination node compares its current sequence number, and the sequence number in the RREQ packet plus one, and then selects the larger one as RREPs sequence number. Upon

receiving a number of RREP, the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with and RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the hole and discards the other RREP packets coming from the other nodes. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination

2. Detection/Prevention of Blackhole Attack: Table II shows a brief description of various approaches to defend against a Blackhole attack along with their limitations.

TABLE-II BLACKHOLE DETECTION/PREVENTION TECHNIQUES

Approach	Description	Limitations
Common Neighbor Listening [25]	Common neighbours used as watchdogs, to detect attack and discover a new route if there is a Blackhole present.	Increased Overhead Works in specific circumstances
Route confirmation Request Reply[26]	Intermediate node requests the next hop to send confirmation message to source. After receiving both, the source decides upon the validity of the path	Doesn't work if 2 consecutive nodes are malicious.
Reply Packet Authenticity[22]	Verifying the authenticity of the node sending RREP, and at the same time waiting for reply packets from 2 or more nodes	Longer time delay
Last Packet Sequence Number[22]	Each node maintains 2 tables with information on 1 last packet sequence number sent to every node. 2 last packet sequence number received from every node.	Malicious node listen to the channel and updates its own table for last packet sequence no.
Dynamic Training Method[27]	Analyzing the difference between the sequence numbers of received reply packets.	False Positives
SAODV[24]	Check path containing repeated next hop node to destination, if there is no repeated node select random path	Increases average end to end delay
MOSAODV[29]	On receiving 1st RREP, the source node waits for a specific time period. During this all received RREP are saved and later on all RREP with very high sequence number discarded.	Rise in average end to end delay Normalized routing overhead
AODV-SABH[28]	To keep information of sequence number of destination node and address of intermediate nodes in RREQ, when a node receives RREP it should check the address of the sender in its local table.	Higher number of control packets ; delay in route discovery process in some scenarios.
DPRAODV[30]	After a specific time interval a threshold sequence number is calculated, if RREP sequence number greater than the threshold, it is considered as a malicious node.	Increases average end-to-end delay and normalized routing overhead.

B. *Wormhole Attack*

The Wormhole attack, is a kind of tunnelling attack which is dangerous and damaging to defend against even though the routing information is confidential, authenticated or encrypted [5].Under this attack two colluding nodes that are far apart are connected by a tunnel giving an illusion that they are neighbours. Each of these nodes receive route request and topology control messages from the network and send it to the other colluding node via tunnel which will then replay it into the network from there [6]. By using this additional tunnel, these nodes are able to advertise that they have the shortest path through them. Once this link is established, the attackers may choose each other as multipoint relays (MPRs), which then lead to an exchange of some topology control (TC) messages and data packets through the

wormhole tunnel. Since these MPRs forward flawed topology information, it results in spreading of incorrect topology information throughout the network [8]. On receiving this false information, other nodes may send their messages through them for fast delivery. Thus, it prevents honest intermediate nodes from establishing links between the source and the destination [10]. More the number of end-to-end paths passing through Wormhole Link, stronger the attack [11].

1. Operation of Wormhole attack: Consider Figure 5 in which node A sends RREQ to node H, and nodes C and G are malicious nodes having an out-of-band channel between them. Node C "tunnels" the RREQ to G , which is legitimate neighbour of H [12]. H gets two RREQ –A-C-G-H and A-B-D-F-H. The first route is shorter and faster than the second, and chosen by H. Since the transmission between two nodes has rely on relay nodes, many routing protocols have been proposed for ad hoc network. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Figure 5. The resulting route through the wormhole may have lower hop count than normal routes [13]. In with this leverage, attackers using wormhole can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DOS attack . The entire routing system in MANET can even be brought down using the wormhole attack [7].Malicious nodes C and G along with the Wormhole link are not visible in the route, and also the Wormhole attacker is hidden from the higher layers.

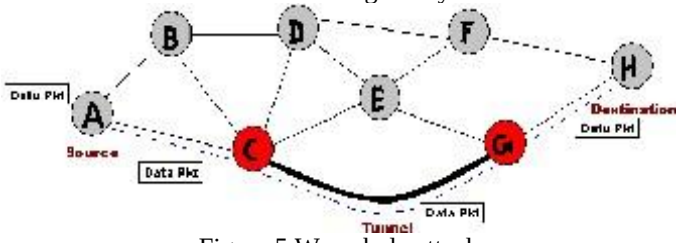

Figure 5 Wormhole attack

2. Detection/Prevention of Wormhole Attack: Various approaches have been proposed to defend against a Wormhole attack. Table III briefly mentions some of them along with their limitations.

TABLE-III WORMHOLE DETECTION/PREVENTION TECHNIQUES

Approach	Description	Limitations
Geographical Leashes[14]	Ensuring that the receiver must be within certain distance from the sender.	Limitations of GPS technology
End-to-end Leashes[15]	Each intermediate node appends time and location information and receiver authentication time and location information of packet using symmetric key.	Limitations of GPS technology
Statistical Analysis[16]	Identifying highest frequency link through analysing relative frequency of each link appearing in obtained routes.	Works only with multipath on demand protocols.
Lite Worp [17]	Instead of 1-hop,2-hop routing information is obtained by nodes, now nodes know their neighbor's neighbour.	Works only for stationary networks.
Localization [18]	Location aware guard nodes send hashed messages, if Wormhole is present, a node detects inconsistencies in the message	Not applicable to mobile networks.
Directional Antennas[19,20]	Each pair of nodes determines the direction of received signals from neighbour, if directions match, relation is set.	Not applicable to network without directional antennas.
Temporal Leashes[14]	Time stamp given for packet	All nodes require tightly synchronized clocks.
Network Visualization[21]	In a sensor network, each sensor senses distance of its neighbours and sends that information to centralized controller topology, with no Wormhole, topology more or less remains flat.	Mobility and terrains not studied for this solution.

C. Grayhole Attack

Grayhole attack is an extension of Blackhole attack in which a malicious node is exceptionally unpredictable. Gray hole attack has two phases [5]. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainty [8]. A Gray hole may exhibit its malicious behavior in different ways [5]. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A Gray hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult and thus degrading network performance [31].

1. Operation of Grayhole Attack: Figure 6 shows a MANET using AODV routing protocol. Node 3 and 5 initially behaves as ordinary nodes and forwards all packets coming from other nodes. After some time, these same nodes (3 and 5) behave maliciously and starts dropping packets send via node 1 and 7 towards the destination. After some time, node 3 and 5 acts as normal nodes. Thus behaving maliciously for a certain period of time. Due to lack of security mechanism in AODV, malicious nodes can perform many attacks just by not following the protocol rules.

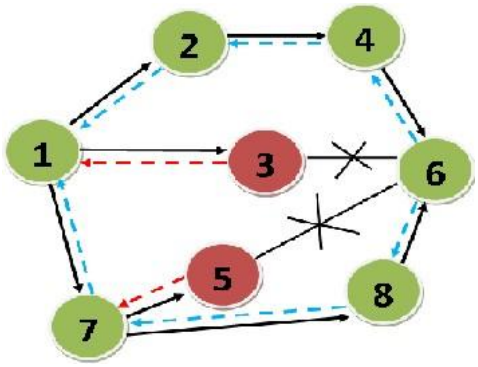

Figure 6 Grayhole attack

2 Detection/Prevention of Grayhole Attack: Table IV briefly describes various approaches for the detection or prevention against a Grayhole attack and limitation of each stated approach.

TABLE-IV GRAYHOLE DETECTION/PREVENTION TECHNIQUES

Approach	Description	Limitations
Creating Proof Algorithm, Check-up Algorithm and Diagnosis Algorithm[31,32]	Each node involved in a session must create a proof that it has received the messages. When source node suspects some misbehaviour, Checkup algorithm checks intermediate nodes. According to the facts returned it traces the malicious nodes by Diagnosis Algorithm.	May not detect all malicious nodes.
End-to-end Checking[33]	Source and destination nodes perform end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a protocol for detecting single or cooperative malicious nodes.	May not work with many malicious nodes. Nodes must be capable of finding their positions when they enter the network.
Flow Conservation[35]	Detecting packet forwarding misbehaviour by the principle of flow conservation and accusation of nodes that are consistently misbehaving. Selecting proper threshold of misbehaviour allows discrimination between well behaved and misbehaved nodes.	It assumes bidirectional communication symmetry in between every direct link between a pair of nodes.
ST-AODV[36]	Trust-based approach that uses passive acknowledgment as it is simplest. Uses promiscuous mode to monitor the channel	It is used only for detecting packet forwarding misbehaviour; monitoring

	that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for.	overall traffic would be a better choice than monitoring only one node's request.
Channel Aware Detection Algorithm[37]	Uses 2 strategies for detecting misbehaving nodes: hop- by- hop loss observation by next hop(downstream node) and traffic monitoring by previous hop (upstream node).	Assumption is made that nodes have no energy constraints and source and destination know the forwarding path and IDs of forwarding nodes.

V. CONCLUSION AND FUTURE WORK

Frequently changing topology of MANET forms the basis for the need of design of most of the routing protocols but security issues have been left ignored. This paper provides brief view about routing as well as security concerns for MANET. We described operations of DoS attacks like Blackhole, Wormhole and Grayhole attacks and surveyed some of the existing solutions for each of them. DoS attacks breach network's security and disrupt network operations. More damage can be done when malicious nodes act cooperatively. Extensive research ought to be carried out for efficient discovery and prevention of these DoS attacks, especially, Grayhole and Blackhole attacks.

REFERENCES

[1] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.
[2] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.
[3] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad- Hoc Networks", International Journal of IT & Knowledge Management, 2010.
[4] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149.
[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.
[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.
[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-InternetCommunication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.
[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.
[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.
[10] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.
[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.
[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.
[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.
[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.
[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.
[16] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi- path," IEEE Wireless Commuunication. and Networking Conference, 2005.
[17] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[18] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.
[19] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium,pp.131-141, 2003.
[20] L.Lazos, R. Poovendran, "Serloc: Secure Range-IndependentLocalization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.
[21] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.
[22] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.
[23] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.
[24] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp.21-26.
[25] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.
[26] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.
[27] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-basedMobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.
[28] Fatima Ameza, Nassima Assam and Rachid Beghdad, "Defending AODV Routing Protocol Against the Black Hole Attack", International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.
[29] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.
[30] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.
[31] Gao Xiaopeng and Chen Wei,"A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", 2007 IFIP International Conference on Network and Parallel Computing – Workshops, 2007, pp.209-214.
[32] Chen Wei, Long Xiang, Bai Yuebin and Gao Xiaopeng,"A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in China, August 2007, pp. 366-370.
[33] Piyush Agrawal, R. K. Ghosh and Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", 2nd international conference on Ubiquitous information management and communication, 2008, pp.310-314.
[34] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", World Congress on Engineering and Computer Science , October 2008, pp. 337-342.
[35] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in MobileAd-Hoc Networks ", Journal of Internet Engineering, vol. 2, no. 1, June 2008, pp. 181-192.
[36] Arshad Jhumka, Nathan Gri_ths, Anthony Dawson and Richard Myers, "An Outlook on the Impact of Trust Models on Routing in Mobile Ad Hoc Networks (MANETs)".
[37] Devu Manikantan Shila, Yu Cheng and Tricha Anjali, "Channel-AwareDetection of Gray Hole Attacks in Wireless Mesh Networks", IEEE Global Telecommunications Conference, Dec. 2009,pp1-6.

