DoS Attacks in Mobile Ad-hoc Networks: A Survey

Rutvij H. Jhaveri
Computer/IT Engineering Department
Shri S'ad Vidya Mandal Institute of Technology
Bharuch 392-001, Gujarat, India
rutusoft@rediffmail.com

Sankita J. Patel
Computer Engineering Department
Sardar Vallabh National Institute of Technology
Surat 395-007, Gujarat, India
sjp@coed.svnit.ac.in

Devesh C. Jinwala
Computer Engineering Department
Sardar Vallabh National Institute of Technology
Surat 395-007, Gujarat, India
dcj@coed.svnit.ac.in

***Abstract*—MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration; as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. In this paper, we will present survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Blackhole attack and Grayhole attack which are serious threats for MANETs. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.**

Keywords-MANETs; Security; DoS Attacks; Wormhole Attack; Blackhole Attack; Grayhole Attack

I. INTRODUCTION

A MANET is a group of mobile nodes wishing to communicate with each other via wireless shared medium; it is a highly adaptable network that can change its form depending on the requirement. As each node has limited communication range, it acts as a router to forward packets to another node. A MANET is rapidly deployable and highly adaptive network; without any pre-defined infrastructure and therefore, line of defense is very unclear. Mobile nodes use radio broadcast medium for communication. Therefore, MANETs have applications in conference meetings, virtual classrooms, automated battlefields, military, rescue systems, voting systems, mobile offices, vehicular computing, electronic payments from anywhere and many more [1].

On the other side, the inherent characteristics of MANET leads to some major issues such as power constraints, radio interference, routing protocols, IP addressing, security, mobility management, service discovery, bandwidth constraints and Quality of Services (QoS) [2]. Among all research issues, security has been a prime concern among researchers. In this paper, we have surveyed some dangerous DoS attacks against MANETs and their proposed solutions given by various research people. The remainder of paper is organized as follows. Section II introduces to routing and type of routing protocols in MANET. Section III addresses security concerns along with types of attacks as well as examples of attacks on different layers of protocol stack. Section IV describes DoS attacks like Wormhole, Blackhole and Grayhole attacks along with proposed solutions for their detection and prevention. Finally conclusion and future directions are given in Section V.

II. ROUTING IN MANETS

As each mobile node works as a router in MANET, routing overhead gets reduced compared to wired networks. Sender and receiver nodes can communicate with each other if and only if they are within the communication range of each other; if they are not, the sender has to send message through intermediate nodes. Due to unpredictable and dynamic nature of MANET, nodes do not have any prior knowledge about topology; therefore, nodes have to determine the topology. A node advertises its presence and listens to advertisements of its neighbors. This is how a node discovers its neighbors as well as ways to reach those. Routing is a big challenge in the environment where nodes are moving very frequently and movement of a host may result in change in the route [1]. Due to these various constraints along with vibrant topology, role of routing protocols is even more challenging.

The primary objective of a routing protocol must be to set up an optimal route that has minimal overhead and consume minimum bandwidth. Types of MANET routing protocols [1, 3] along with their characteristics and examples are shown in TABLE I.:

TABLE I. ROUTING PROTOCOLS

Type	Characteristics	Examples
Proactive (Table-driven)	• Routes are computed prior to requirement • Periodical updation and distribution of routing information	DSDV, OLSR, WRP, CGSR, FSR
Reactive (On-demand)	• Routes are discovered, when demanded, by flooding route request • No requirement of distribution of routing information	AODV, DSR, ACOR, ABR
Hybrid	• Combination of good characteristics of proactive and reactive protocols	TORA, ZRP, ARPAM, OORP, HSR, CGSR, LANMAR

The main advantage of proactive protocols is that a route can be selected immediately without any kind of holdup; but maintaining large amount of data for routing information with higher bandwidth and slow reaction on failures are major drawbacks. Reactive protocols consume less bandwidth and

effective in route maintenance; but they require higher time for route discovery and sometimes excessive flooding may lead to network congestion. Efficiency of hybrid protocols may vary with number of nodes and the amount of traffic decides the reaction to demand.

III. SECURITY CONCERNS

Due to lack of trusted centralized administration, limited bandwidth, limited power, wireless links, dynamic topology and easy eavesdropping MANETs are more susceptible to security attacks than existing conventional networks [4]. A network's goals are availability, integrity, confidentiality, authentication and non-repudiation. An attacker can violate them by passively or actively attacking on MANETs [5]. TABLE II. shows the characteristics and examples of active and passive attacks. Both active and passive attacks can be launched on any layer of the network protocol stack. Table III. [6, 7] shows some examples of attacks on different layers.

TABLE II. ROUTING ATTACKS

Type of Attack	Characteristics	Examples
Passive Attacks	• Obtains information without disturbing normal network operation • Difficult to detect	Traffic analysis, traffic monitoring and eavesdropping
Active Attacks	• Can be internal (attacker within the network) or external (attacker outside the network) • Can disturb network operation by modifying or deleting information, injecting a false message or impersonating a node	Modification, impersonation, fabrication, jamming and message replay

TABLE III. ATTACKS ON DIFFERENT LAYERS OF PROTOCOL STACK

Layer	Examples of Attacks
Application Layer	• Repudiation
Transport Layer	• Session hijacking
Network Layer	• DoS attacks: Wormhole, Blackhole, Grayhole, Byzantine, Resource Consumption attack, Rushing attack • Information Disclosure • Routing attacks: Routing table overflow, Routing table poisoning, Packet replication, Route cache poisoning
Multiple Layers	• Denial of Service (DoS), SYN flooding, Impersonation, Device tampering

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

DoS attacks are active attacks in which malicious nodes generate false messages in order to disrupt the network's operations or to consume other nodes' resources. We will discuss Wormhole, Blackhole and Grayhole attacks as well as existing solutions to detect and fight against them.

A. Wormhole attack

The Wormhole attack is a kind of tunneling attack which is extremely dangerous and damaging to defend against even though the routing information is confidential, authenticated or encrypted [5]. It can be mounted without prior knowledge of routing protocols and without compromising nodes [8]. It is relatively easy to deploy but exceedingly hard to detect. Usually Wormhole attack is launched by two malicious nodes (worms) connected via a high-speed wired or wireless link called Wormhole link or tunnel. Nodes outside each other's communication range have to communicate via intermediate nodes in a multi-hop way. Worms are placed at very powerful positions in the network. They encapsulate data packets and falsify the route lengths [6]. One worm records packets at one location and replays them to another location to peer worm, giving impression to nodes in both groups that they are immediate neighbors [8]. Many packets in the network would be delivered through these worms. If the attacker carries out the tunneling reliably and truthfully then it can work very efficiently in connecting the network [6], but the worms can drop delivered messages and acquire statistical data of traffic by investigating message traffic [9]. To minimize delay, the attacker may forward each bit through the Wormhole link without waiting for the entire packet to be received [6]. It is generally assumed that Wormhole attacks do not alter integrity of captured packets [10]. More the number of end-to-end paths passing through Wormhole link, stronger the Wormhole attack [11].

1) Operation of Wormhole Attack: As shown in Figure 1., two malicious nodes X and Y launch the Wormhole attack on the MANET. X and Y are connected via a high-speed Wormhole link that tunnels traffic between nodes S and D [12]. As mentioned in [13], when node S wishes to communicate with node D, normally it takes multiple hops for a packet to travel between them. Though in the presence of worms X and Y, S and D start believing that they are immediate neighbors. Packets traveling through Wormhole link travel faster to the destination than packets traveling through multiple hops in the MANET. X and Y do not alter the packet header and falsify the route lengths. Thus, Wormhole attack can prevent normal intermediate nodes from correctly incrementing the metric used to determine path lengths [6]. Packets received by X are replayed through Wormhole link to Y and vice versa. X and Y can now selectively drop data packets or analyze traffic and disrupt the network's communication. Malicious nodes X and Y along with the Wormhole link are not visible in the route; and also the Wormhole attacker is hidden from the higher layers. Therefore, detection of Wormhole attack is exceedingly tough.

2) Detection/Prevention of Wormhole Attack: Table IV. shows brief discription of various approaches for detection or prevention against a Wormhole attack and their limitations.

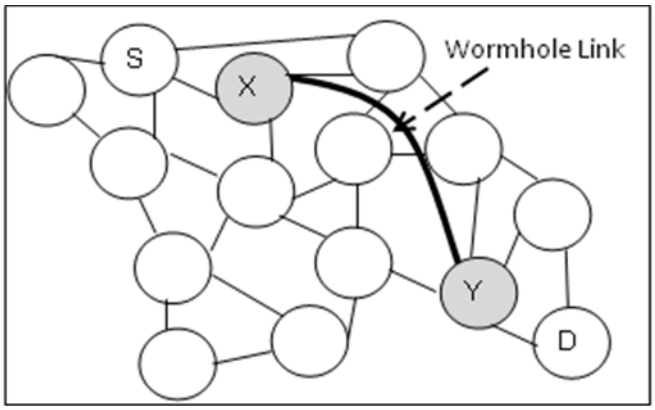


Figure 1. Wormhole attack

TABLE IV. WORMHOLE DETECTION/PRVENTION TECHNIQUES

Approach	Description	Limitations
Geographical Leashes[14]	Ensuring that the receiver must be within certain distance from the sender	Limitations of GPS technology
Temporal Leashes[14]	Time stamp given for packet	All nodes require tightly synchronized clocks
End-to-end Leashes [15]	Each intermediate node appends time and location information and Receiver authenticates time and location information of a packet using symmetric key	Limitations of GPS technology
Statistical Analysis [16]	Identifying highest frequency link through analyzing relative frequency of each link appearing in obtained routes	Works only with multimpath on demand protocols
LiteWorp [17]	Instead of one-hop, two-hop routing information is obtained by nodes; now nodes know their neighbors' neighbor	Works only for stationary networks
Localization [18]	Location Aware Guard Nodes (LAGNs) 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 neighbor; if directions match, relation is set	Not applicable to network without directional antennas
Network Visualization [21]	In a sensor network, each sensor senses distance of its neighbors and sends that information to centralized controller from which it calculates topology; With no Wormhole, topology more or less remains flat	Mobility and terrains not studied for this solution

B. *Blackhole attack*

Blackhole attack is another type of DoS attack that generates and disseminates fabricated routing information. As mentioned in [22], a malicious node, exploiting the flooding-based routing protocol, advertises itself as having a valid shortest route to the destined node. If the malicious node replies to the requesting node before the actual node replies, a bogus route will be created. Therefore packets are not forwarded to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, absorbs network traffic [23].

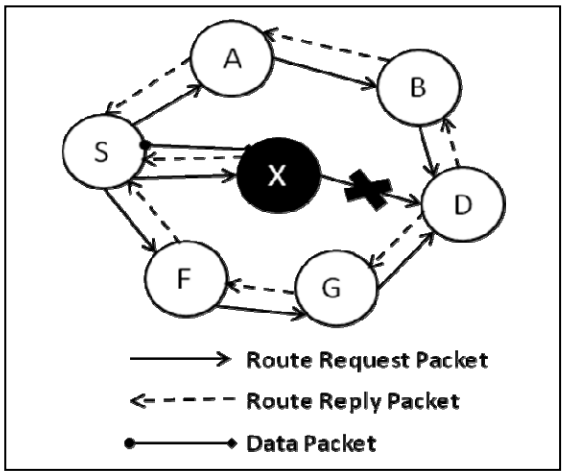


Figure 2. Blackhole attack

1) Operation of Blackhole Attack:

An example of Blackhole attack against AODV protocol (Ad-hoc On demand Distance Vector) is shown in Figure 2. [24]. Suppose source S wants to communicate with node D. S initiates route discovery process by broadcasting route request packets (RREQ) to its neighbors. The destination node D or any intermediate nodes having fresh route to the destination can give reply by sending reply packet (RREP) to S. Considering no intermediate nodes have a fresh route to D, they forward request packets towards destination. As X is a malicious node, it doesn't forward the request packet ahead; instead, it falsely replies to S indicating that it has a valid fresh route to D. Thus, reply packet from X reaches to S ahead of reply packets from other neighbors of S. Therefore, S considers sending packets to D via X considering that X has a shortest route to D. Now X absorbs all packets forwarded from S to D. This is how a Blackhole attack is setup.

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

TABLE V. BLACKHOLE DETECTION/PREVENTION TECHNIQUES

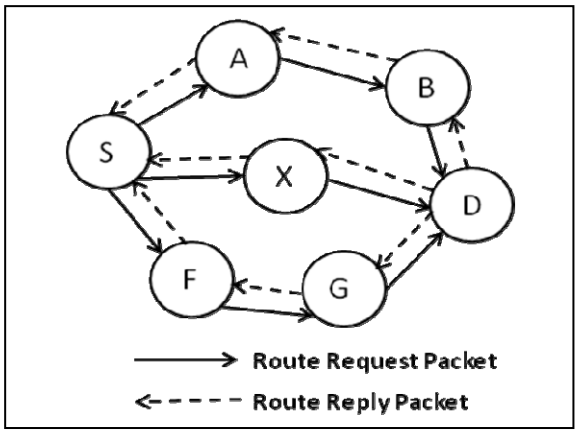
Approach	Description	Limitations
Reply Packet Authenticity [22]	Verifying the authenticity of node sending reply packet and wait for reply packets from more than two nodes	Longer time delay
Last-Packet-Sequence-Numbers [22]	Every node keeps two additional small-sized tables: one to keep last-packet-sequence-numbers sent to every node and second to keep last-packet-sequence-numbers received from every node	The malicious node can listen to the channel and update the tables for the last packet sequence number

Approach	Description	Limitations
Common Neighbor Listening [25]	Using common neighbors, acting as watchdogs, to detect attack and discover a new route if there is a Blackhole present	Adds some routing control overhead and works in specific circumstances
Route Confirmation Request-Reply [26]	The intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and confirmation message, the source determines the validity of path according to its policy	Doesn't work if two consecutive nodes are malicious
Dynamic Training Method [27]	Analyzing differences between 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
AODV-SABH [28]	To keep information of sequence number of destination node and addresses 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
MOSAODV [29]	After receiving first RREP, the source node waits for a specific time period; for this period source node saves all received RREP message in a table; Source node discards all RREPs having very high sequence number	Rise in average end-to-end delay and normalized routing overhead; Heuristic approach
DPRAODV [30]	After specific time interval a threshold sequence number is calculated; if RREP has sequence number greater than the threshold, it is considered as a malicious node	Increases average end-to-end delay and normalized routing overhead
Data Routing Information (DRI) and cross checking [31]	The intermediate node generating RREP sends next hop node and its DRI table entry; cross checking is done on intermediate node; the source node uses reliable node to send the packet	Cross checking cost is more
Further Request and Further Reply [32]	Each intermediate node sends back the next hop information while sending back an RREP. When the source node receives the RREP, it extracts the next hop information from it then sends a Further Request to the next hop to verify that it has a route to the intermediate node who sends back the Further Reply message, and that it has a route to the destination node.	May not work against cooperative Blackhole attacks
Voting System [33]	Each node maintains an estimation table containing status information about nodes within the power range. One node detects suspicious node and notifies that to neighbors. The nodes cooperatively vote for the consideration of the suspicious node as Blackhole.	Cannot detect cooperative Blackholes; the voting system is not considered good
Data Routing Information (DRI) and cross checking using FREQ and FREP [34]	It discovers the secure route between source and destination by identifying and isolating cooperative Blackhole nodes; This approach uses modified version of AODV; It introduces DRI table and cross checking using Further Request (FREQ) and Further Reply (FREP). Works better than other similar kind of approaches	May not work with more percentage of Blackhole nodes

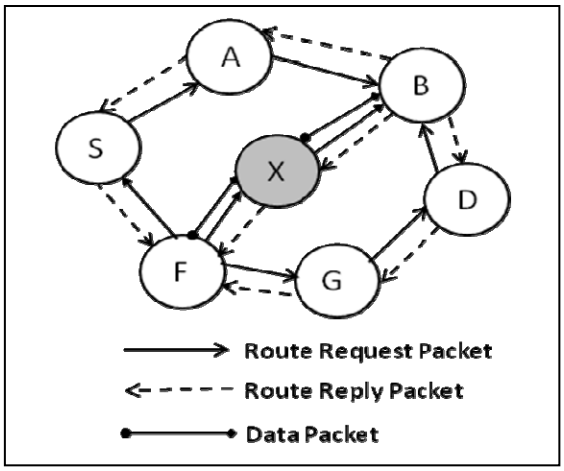
C. *Grayhole attack*

Grayhole attack is an extension of Blackhole attack in which a malicious node's behavior is exceptionally unpredictable. There are three types of Grayhole attacks [5]. In first, the malicious node may drop packets from certain nodes while forwards all other packets. In second type, a node may behave maliciously for a certain time, but later on it behaves just like other ordinary nodes. Third type of attack is the combination of both attacks i.e. the malicious node may drop packets from specific nodes for certain time only, later it behaves as a normal node. Due to these characteristics, detection of Grayhole attacks is not an easy task. A Grayhole attack can disturb route discovery process and degrade network's performance [35].

1) Operation of Grayhole Attack: Figure 3. (a) shows a MANET using AODV routing protocol. Node X intially behaves as an ordinary node and forwards all packets from source S to the specified destination D. After some time, as shown in Figure 3. (b), node X behaves maliciously and starts dropping packets sent by source S to the destination D. After some time, X acts as a normal node as earlier.Thus, X behaves maliciously for certain time period. As AODV doesn't have any security mechanism, malicious nodes can perform many attacks just by not following the protocol rules.



(a)



(b)

Figure 3. Grayhole Attack

2) Detection/Prevention of Grayhole Attack: Table VI. briefly describes various approaches for detection or prevention against a Grayhole attack and their limitations.

TABLE VI. GRAYHOLE DETECTION/PREVENTION TECHNIQUES

Approach	Description	Limitations
Creating Proof Algorithm, Check up Algorithm and Diagnosis Algorithm [35,36]	Each node involved in a session must create a proof that it has received the message; When source node suspects some misbehavior, Checkup algorithm checks intermediate nodes; According to the facts returned by the Checkup algorithm, it traces the malicious node by Diagnosis algorithm	May not detect all malicious nodes
End-to-end Checking [37]	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
Prelude and Postlude Messaging [38]	Before sending any block, source sends a prelude message to destination to alert it; neighbors monitor flow of traffic; after end of transmission, destination sends postlude message containing the number of packets received. If the data loss is out of tolerable range, initiate the process of detecting and removing all malicious nodes by aggregating response from monitoring nodes and the network	Analysis of the proposed solution has not been done
Flow Conservation [39]	Detecting packet forwarding misbehavior by the principle of flow conservation and accusation of nodes that are consistently misbehaving. Selecting proper threshold of misbehavior allows discrimination between well-behaved and misbehaved nodes; it also provides robustness against various grades of mobility in a network that is affected by Grayhole / Blackhole attacks.	Only packet forwarding misbehavior is addressed; It assumes bidirectional communication symmetry in every direct link between a pair of nodes; assumes reliability of MAC layer protocol; assumes all nodes adapted with wireless interfaces supporting promiscuous mode operation.
ST-AODV [40]	Trust-based approach that uses passive acknowledgement as it is simplest; Uses promiscuous mode to monitor the channel that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for; thus, a node can ensure that packets it has sent to a neighboring node for forwarding are indeed forwarded; routing choices are made based on trust as well as hop-count, such that the selected next hop gives the shortest trusted path.	It is used only for detecting packet forwarding misbehavior; monitoring overall traffic would be a better choice than monitoring only one node's requests.
Channel-aware Detection Algorithm [41]	It uses two 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.
Simple acknowledgement and flow conservation [2]	One-way hash code is added to the data packets; when receiver receives packet, it checks the correctness of it by finding match of hash code; for correct data packet, it sends ACK to sender which checks the ACK is received within specific time; for incorrect packet receiver sends CONFIDENTIALITY LOST through intermediate nodes and sender switches to alternative intermediate node to send packets.	The solution is not tested with higher density of nodes and adds to the routing overhead.
Anti-Blackhole Mechanism (ABM) [42]	ABM estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node; All	It is assumed that a node ID cannot be forged, and a block

Approach	Description	Limitations
	nodes perform ABM; with the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node is not the destination and never broadcasts a RREQ for a specific route, but forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby node's suspicious node table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected node to all nodes in the network in order to isolate the suspicious node cooperatively.	message, sent by an IDS node, cannot be modified

V. Conclusion And Future Work

Designs of most of the routing protocols are based on the requirement of frequently changing topology of the MANET, 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 Wormhole, Blackhole 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 Blackholeattacks.

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-Internet Communication", 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-Independent Localization 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-based Mobile 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] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard," Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".

[32] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing security in Wireless Ad-hoc Network",IEEE Communications Magazine, Issue 40, 2002, pp 70–75.

[33] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang,"A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network" , Springer-Verlag Berlin Heidelberg, 2007.

[34] Hesiri Weerasinghe, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July, 2008, pp: 39-54.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks ", Journal of Internet Engineering, vol. 2, no. 1, June 2008, pp. 181-192.

[40] 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)".

[41] Devu Manikantan Shila, Yu Cheng∗ and Tricha Anjali, "Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks", IEEE Global Telecommunications Conference, Dec. 2009, pp. 1-6.

[42] Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications 2010.