ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

A Detail Qualitative Survey on Attacks in Mobile Ad-hoc Networks (MANET)

Himanshi[1], Mintu Singh[2]

M-Tech. Student, Department of CSE, Echelon Institute of Technology, Faridabad, India[1]

Assistant Professor Department of CSE, Echelon Institute of Technology, Faridabad, India[2]

Abstract: Mobile ad hoc networks (MANET) has risen as a major next generation wireless networking technology. This network is a network of mobile nodes with dynamic structure. Here each node acts as a router for forwarding data to other nodes. Due its dynamic nature, security has become a primary concern to provide protected communication between different nodes in ad hoc networks. There are a number of challenges in security design as ad hoc network is a decentralized network. There are five layers in MANET and each of these layer is vulnerable to various attacks. In this paper we discuss about various attacks and their protection mechanisms.

I. INTRODUCTION

Wireless networks are classified into two broad categories: infrastructure less networks and infrastructure based networks. The infrastructure based networks can make the use of fixed base stations which are responsible for coordinating communication among two or more mobile hosts. Infrastructure less wireless networks is a type of network of mobile nodes with no central coordinator. MANET (Mobile ad-hoc network) comes under the category of infrastructure less or non-infrastructure wireless networks.

The term ad-hoc means temporary i.e. a mobile ad-hoc network is a temporary network of various mobile nodes without any central coordinator [1]. These networks do not depend on any hardware. A MANET is a self-governing network in which each node acts as a router to forward message to other node that are not within the same communication range. MANET follows a dynamic topology because every node always moves arbitrarily in the network [2].

Therefore, a node can change its link to other node frequently. Because of dynamic topology MANET has various applications such as in military area, rescue operations, natural disaster recovery etc. apart from these MANET can also install in the office, home or a small area of city. Though, MANET supports mobility and portability but is more vulnerable and susceptible to various types of security attacks. MANET not only inherits all the security attacks found in both wired and wireless networks, but it also introduces some of the security attacks unique to itself.

With the knowledge of some commonly used attacking schemes, a researcher might have a better understanding of how mobile ad hoc networks could be susceptible to the attackers, and thus leads to the development of more reliable security measures in protecting them [2]. The main aim of this study is to inspect some of the important issues that might be related to security attacks in MANET and some of the existing detection and mitigation schemes [3].

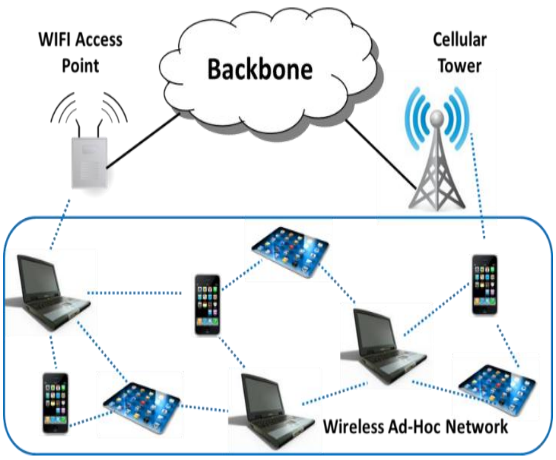

Figure: 1 Mobile Ad-hoc Networks

II. ATTACKS IN MANETS

Mobile ad-hoc networks are vulnerable to numerous attacks not only from outside but also from inside i.e. within the network. The attacks in MANET are divided into two major categories:

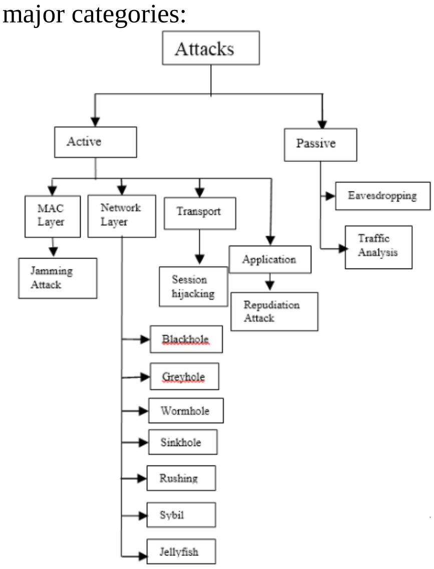

Fig :Types of attack

DOI 10.17148/IJARCCE.2015.4514

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

A. Active Attacks

Active attacks disturb the operation of communication in the network. Anactive attack could stop the message flow between the nodes. An active attack can modify the data packet or drop the packet in the network. Hence active attacks disturb the normal functionality of a MANET.

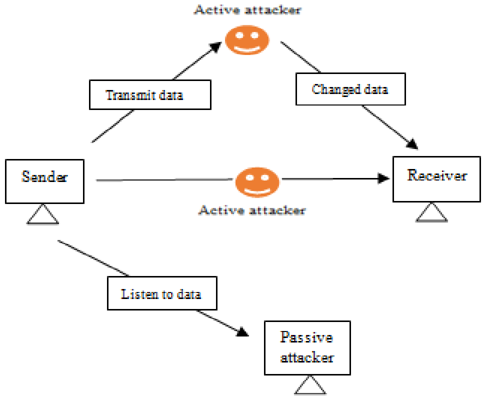

Fig: Active - Passive attacks

Attacks at MAC Layer

1.) Jamming attack

Jamming attack is a type of denial of service attack. Jamming attack uses the term jammer. Jammer can be defined as an individual entity which intentionally blocks the methods of legal wireless communication. It comes under active attack due to its actions. In jamming attack, a radio signal is jammed or interfered which causes the message to be lost or corrupted. The attacker node having a powerful transmitter causes that the generated signal will be strong enough to damage the communications and can easily crush the targeted signal [5]. This attack is originated after determining the communication frequency.

Attacks at Network Layer

1.) Blackhole attack

In this attack, attacker node announces that it has an optimum route to the node whose packet it wants to use. On receiving side, attacker node sends a fake reply with extremely short route. If the node has been able to make its place between the communicating nodes, then it can do anything with the packets passing between them [1]. A black hole node acts as having a path with the highest sequence number to the destination. The black hole node falsely advertises the shortest path to the destination node in order to absorbs data packets and drop them [1].

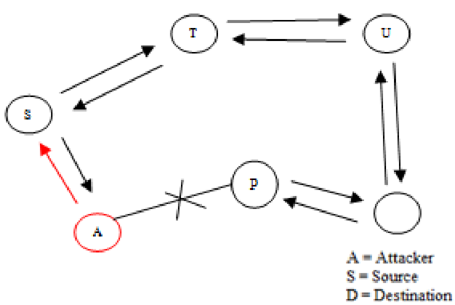

Fig :Blackhole attack

2.) Greyhole attack

Greyhole attack is a special kind of blackhole attack. In this attack, an attacker becomes the part of the routes in the network i.e. captures the route then drops data packets selectively [2]. One can't predict the probability of losing data packets.In greyhole attack, attacker node first agrees to forward packets and then refuses to do so, which leads to dropping of data packets.

The Gray Hole attack has two phases: In the first phase, an attacker node exploits the AODV protocol to act as having a valid route to the destination node, with the goal of interrupting data packets, even though the route is spurious. In the second phase, the attacker node drops the interrupted data packets with a certain probability. Greyhole attack is more difficult to detect as compared to black Hole attack in which the attacker node drops the received data packets with certainty.

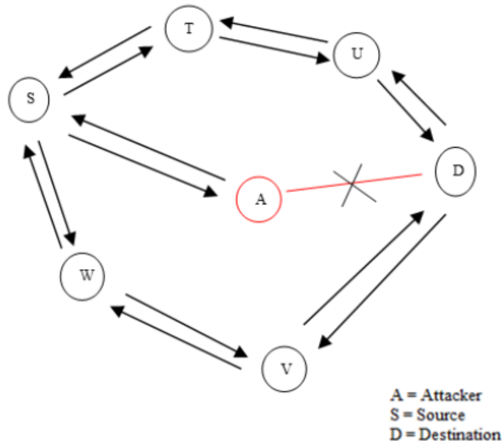

Fig :Greyhole Attack

3.) Wormhole

In this type of attack, two attacker nodes are present in the network which creates a tunnel. An attacker node receives the data packet at one point in the network and forward it to another attacker node. The tunnel exist between two attacker nodes is called wormhole. Wormhole places the attacker nodes in a very powerful position compared to other nodes in the network. The attacker node could use this position in a number of ways. In wormhole attack, it copies the data packets at one location and replays them without any changes at different location or within the same network.

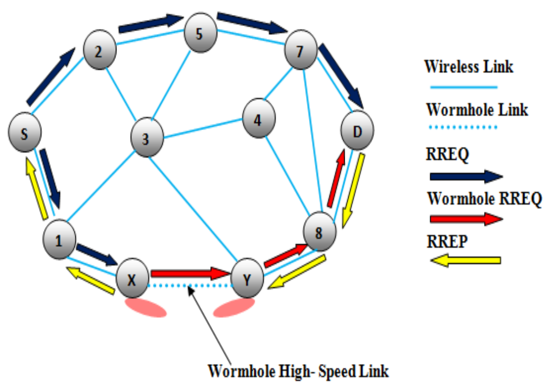

Fig :Wormhole Attack

DOI 10.17148/IJARCCE.2015.4514

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

4.) Sinkhole attack

In this attack, an attacker node provides wrong routing information in order to presents itself a specific node and hence receives the whole network traffic. Once receiving the whole network traffic complicated packet traffic it modifies secret information such change the data or drop the packet to make network complicated. An attacker node tries to attract the secure data from all neighboring nodes.

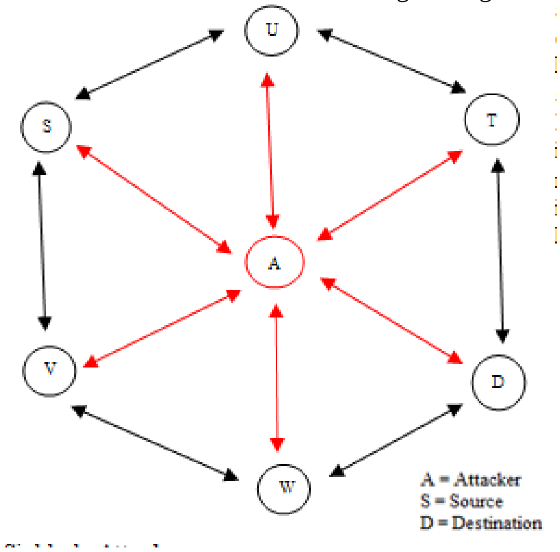

Fig : Sinkhole Attack

5.) Rushing Attack

Rushing attack can also be known as a denial of service attack or novel attack. In rushing attack, an attacker node receives a route request packet from the source node and immediately flood it throughout the network before other nodes which also receive the same route request packet. These attacks are generally against the on-demand routing protocols.

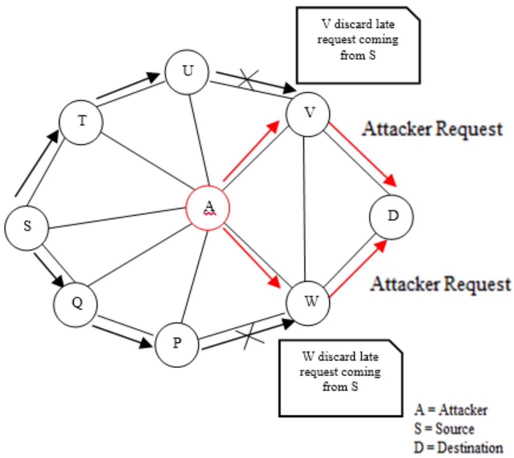

Fig : Rushing Attack

6.) Sybil Attack

In MANET the transmission medium for data packets is air and they doesn't have a centralized node to control the network. So the routing is based on some unique node address. This property of MANET can be used by the attacker for using fake identities. This means the attacker can either use a random identity or the identity of legitimate node. This type of attack is known as Sybil attack.

In Sybil attack, an attacker may create multiple fake identities. The attacker node may present itself as a large number of nodes instead of a single node. These fake identities are called Sybil nodes.This attack may cause a lot of data packets to be routed towards the fake nodes.

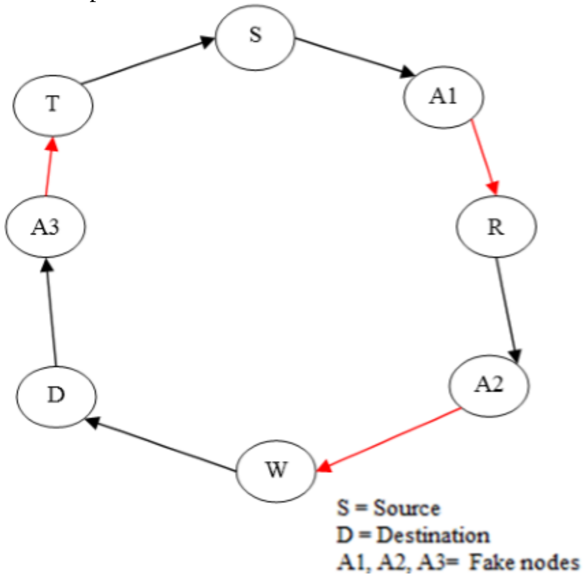

Fig ; Sybil attack

7.) Jellyfish Attack

Jellyfish attack generally comes under the passive attack and also a type of denial of service attack. Jellyfish attack produces delay during the transmission and reception of data packets in the network. This attack is difficult to detect. Jellyfish attack is same as the blackhole attack with the only difference that is in blackhole attack attacker drops all data packetsbut in jellyfish attack node produces delay during forwarding of data packets.

Attacks at transport Layer

1.) Session Hijacking

In this type of attack, the attacker node tries to obtain secure data which could be password, secret key etc. and other useful information. An attacker creates a fake ip address and obtains the correct sequence number. This attack aims at collecting secret data about the nodes.

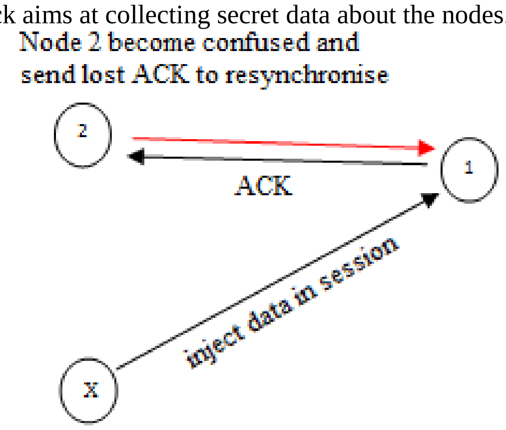

Fig : Session Hijacking

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Attacks at Application Layer

1.) Repudiation attack

Repudiation means denial of transmitting or receiving the data packet. In this type of attack, either a sender may deny that he send the packet or a receiver deny that he receives a data packet.

B. Passive Attacks

A passive attack is an unauthorized listening to the network. It does not change the data transmitted within the network. A passive attacker obtains the data exchanged in the network without disturbing the operation of communication.

Passive attack is difficult to detect because of the network operation itself does not get affected. These attacks can be controlled by using powerful encryption algorithm to encrypt the data which is being transmitted.

Passive attacks are further classified into two categories:

1.) Eavesdropping

Eavesdropping is an interception and reading of messages by an unauthorized receiver. The unintended receiver can easily intercept the communication which is on wireless medium by tuning up to proper frequency. The main aim of eavesdropping which is kept secret during the communication. The secret information can be private key, public key, password.

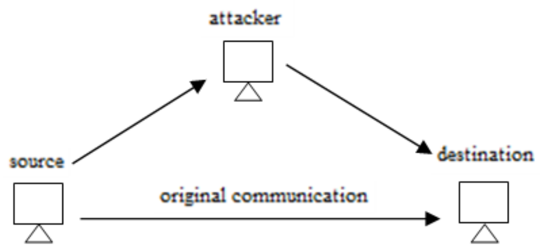

Fig : Eavesdropping

2.) Traffic Analysis

In this attack, for an attacker data packets and traffic patterns both are important. The attacker can obtain the confidential information about network topology by analyzing the traffic pattern. Using traffic analysis attack, an attacker may find about network topology, location of nodes, source and destination nodes.

III. ATTACK DETECTION AND PREVENTION TECHNIQUES

TABLEI. BLACKHOLE DETECTION/PREVENTION TECHNIQUES

Approach	Description	Limitations
Reply Packet Authenticity [22]	Verifying the authenticity of node sending reply packet andwait for reply packets from more than two nodes	Longer time delay
Last-Packet-Sequence-Numbers [23]	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
Common Neighbor Listening [25]	Using common neighbors, acting as watchdogs, to detect attack and discover a new route if there is a Black hole present between source and destination by identifying and isolating cooperative Black hole nodes;	Adds some routing controloverhead and works in specific circumstances
Information (DRI) and Cross checking using FREQ and FREP [26]	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	with more percentage of Black hole nodes

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

	similar kind of approaches	
Route Confirmation Request-Reply [27]	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 [28]	Check path containing repeated next hop node to destination; if there is no repeated node, select random path	Increases average end-to end delay
AODVSABH [29]	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 [30]	After receiving	Rise in average end-to-end

	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	delay and normalized Routing overhead; Heuristic approach
DPRAODV [31]	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
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 Black hole.	Cannot detect cooperative Black holes; the voting system is not considered good

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Approach	Description	Limitations
Channel-aware Detection Algorithm [41]	It uses two strategies for detecting misbehaving nodes: hop-by-hop loss observation by next hop (downstream node) andtraffic 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.
Prelude and Postlude Messaging [38]	Before sending any block, source sends a prelude message todestination 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 frommonitoring nodes and the network	Analysis of the proposed solution has not been done
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
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
Simple acknowledge-ment 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.
End-to-end	Source and destination nodes	May not work with many

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Checking [37]	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	Malicious nodes; nodes must be capable of finding their positions when they enter the network

IV. CONCLUSION AND FUTURE WORK

The dynamic nature of MANET makes it vulnerable to attacks at different layers. One of the mostly attacked MANET layer is network layer. So, there is a need for secure environment for transmission of secure communications. In this paper, I have done a survey on network layer attacks and their possible detection mechanism. In future there can be several ways to defeat these protection mechanisms. So this is a further more potential area of research in which more powerful detection mechanisms can be invented.

REFERENCES

[1]. 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.

[2]. 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.

[3]. 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.

[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

[16]. Attacks in Mobile Ad Hoc Networks”, Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[17]. L. Qian, N. Song, and X. Li, “Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath,” IEEE Wireless Commuunication. and Networking Conference,

[18]. 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.

[19]. 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.

[20]. L. Hu and D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks”, 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[21]. L.Lazos, R. Poovendran, “Serloc: Secure Range-Independent Localization for Wireless Sensor Networks”,ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[22]. W. Wang, B. Bhargava, “Visualization of Wormholes in sensor networks”, ACM workshop on Wireless Security, pp. 51-60, 2004.

[23]. Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACMSE, April 2004, pp.96- 97.

[24]. Anu Bala, Munish Bansal and Jagpreet Singh, “Performance Analysis of MANET under Blackhole Attack”, First International Conference on Networks & Communications, 2009, pp. 141-145.

[25]. 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.

[26]. Geng Peng and Zou Chuanyun,”Routing Attacks and Solutions in Mobile Ad hoc Networks”, International Conference on Communication Technology, November 2006, pp. 1-4.

[27]. S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks”, International Conference on Parallel Processing Wowrkshops, August 2002.

[28]. 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.

[29]. Nadia Qasim, Fatin Said, and Hamid Aghvami, “Performance Evaluation of Mobile Ad Hoc Networking Protocols”, Chapter 19, pp. 219-229.

[30]. 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.

[31]. 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.