A Detail Qualitative Survey on Denial of Service Attacks in Mobile Ad-hoc Networks

Neeti Yadav

M-Tech Student & Department of CSE & Delhi College of Technology & Management
Palwal, Haryana, India

***Abstract*— Mobile ad-hoc networks are more vulnerable to security attacks due to their unique characteristics such as dynamic topology, no fixed infrastructure, resource limitations and multi-hop scenario. 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, Black hole attack and Gray hole 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.**

***Index Terms*— MANETs; Security; DoS Attacks; Wormhole Attack; Black hole Attack; Gray hole Attack**

I. INTRODUCTION

MANET is an autonomous and decentralized wireless system. It is also called self organized, infrastructure less networks. Each node not only operates as an end system, but also acts as a router to forward packets. Nodes cooperate with each other to route the control and the data packets from source to destination. Routing in MANET is classified in two types proactive (table driven) and reactive (On-Demand). In a proactive routing protocol, nodes periodically exchange routing information with other nodes. In a reactive routing protocol, nodes will exchange routing information only when needed.

Due to dynamic changing topology, open medium, and no clear line defense attacks on MANET 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.

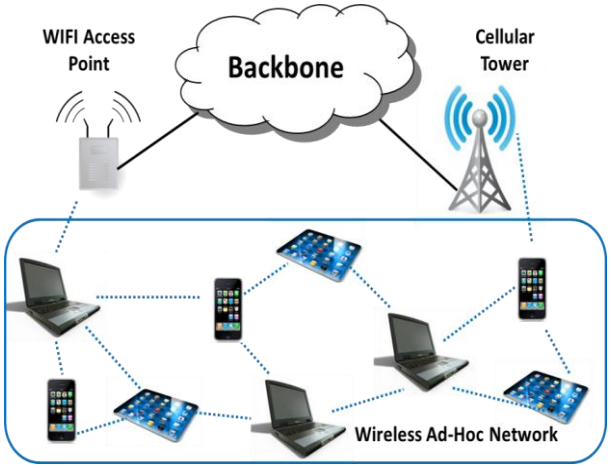

Figure: 1 Mobile Ad-hoc Networks

Section II introduces to routing attacks 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, Black hole and Gray hole attacks along with proposed solutions for their detection and prevention. Finally conclusion and future directions are given in Section V.

II. SECURITY ATTACKS

Ad hoc wireless networks are highly vulnerable to security attacks as compared to other wired networks. This is due to the following characteristics: insecure operating environment, physical vulnerability, shared broadcast radio channel, lack of central authority, limited availability of resources and lack of association [7]. In Ad hoc wireless networks, attacks are classified into two broad categories [15]:

- **Passive attack**-A passive attack just attempts to snoop the valuable information from the network and does not disrupt the operation of the network. Confidentiality is violated if the data is interpreted through snooping.
- **Active attack**-It attempts to alter or destroy the data, gain authentication thereby disrupting the functioning of the network.

III. 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

ISSN: 2278 – 1323

discuss Wormhole, Black hole and Gray hole 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.

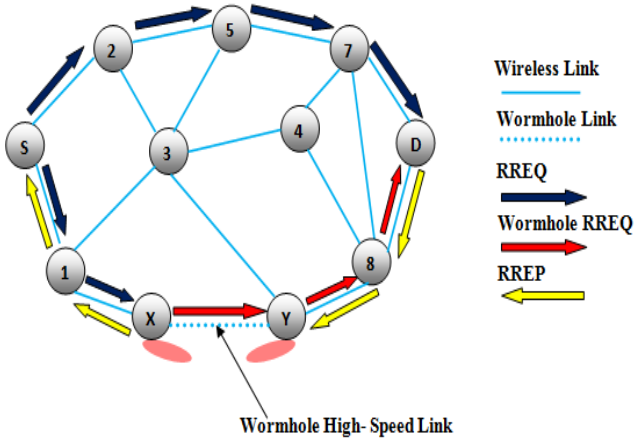

Figure: 2 Wormhole Attack

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].

Detection/Prevention of Wormhole Attack:

Table I. shows brief description of various approaches for detection or prevention against a Wormhole attack and their limitations.

Table I. 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 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 multi path on demand protocols
Statistical Analysis [17]	Identifying highest frequency link through analyzing relative frequency of each link appearing in obtained routes	Works only with multipath on demand protocols
Temporal Leashes[18]	Time stamp given for packet	All nodes require tightly synchronized clocks
LiteWorp [19]	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	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. Black Hole Attack:

In black hole attack, a malicious node sends false routing information and claiming that it has an original route and causes other good nodes to route data packets through the malicious one [16]. All traffic will be routed through the attacker, and the attacker can misuse or discard the traffic

Detection/Prevention of Black hole Attack:

Various approaches have been proposed to defend against a Black hole attack; Table II. Briefly mentions some of them along with their limitations.

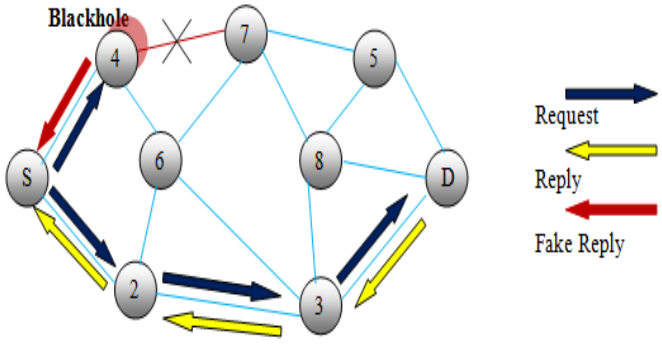

Figure: 3 Black Hole Attack

Table. II Black hole Detection/Prevention Techniques

Approach	Description	Limitations
Reply Packet Authenticity [2]	Verifying the authenticity of node sending reply packet an wait for reply packets from more than two nodes	Longer time delay
Last-Packet-Sequence-Numbers [6]	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[5]	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 control overhead and works in specific circumstances
Information (DRI) and Cross checking using FREQ and FREP [9]	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	with more percentage of Black hole nodes
Route Confirmation Request-Reply [10]	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 [17]	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 [21]	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 [22]	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 [24]	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 [22]	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

C. Gray Hole Attack:

Gray hole attack is an extension of Black hole attack in which a malicious node's behavior is exceptionally unpredictable. There are three types of Gray hole 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 Gray hole attacks is not an easy task. A Gray hole attack can disturb route discovery process and degrade network's performance [25].

ISSN: 2278 – 1323

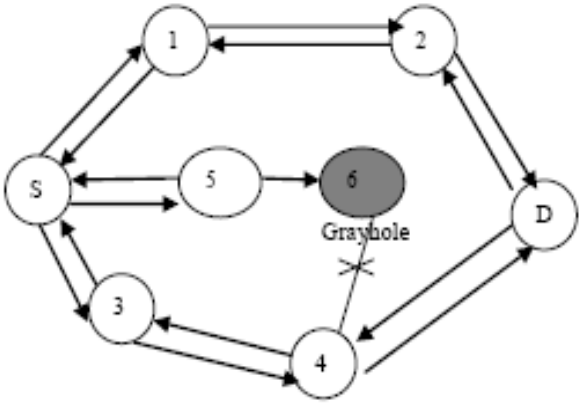

Figure: 4 Gray Hole Attack

Detection/Prevention of Gray hole Attack*:*
Table III briefly describes various approaches for detection or prevention against a Gray hole attack and their limitations.

Table: III Detection/Prevention of Gray hole Attack

Approach	Description	Limitations
Channel-aware Detection Algorithm [11]	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.
Prelude and Postlude Messaging [18]	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
Creating Proof Algorithm, Check up Algorithm and Diagnosis Algorithm[19]	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 [20]	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 acknowledgement and flow conservation [23]	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 Checking [27]	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 the enter the network

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, Black hole and Gray hole 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, Gray hole and Black hole attacks.

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

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

[29] 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.

[30] 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.

ISSN: 2278 – 1323