Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview

Swati Jain[1], Naveen Hemrajani[2]

[1]M.Tech Scholar, Department Of Computer Science & Engineering
Suresh Gyan Vihar University, Jaipur, Rajasthan, India

[2]Professor, Department Of Computer Science & Engineering
Suresh Gyan Vihar University, Jaipur, Rajasthan, India

Abstract: ***As the increase of wireless networks, use of mobile phones, smart devices are gaining popularity so the adhoc network is also an uprising field. Each device in a MANET is free to move independently in any direction, linking to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply etc. This paper describes the features, application, and vulnerabilities of mobile ad hoc network also presents an overview and the study of the attacks and their mitigation in routing protocols.***

Keywords: MANET, Wireless Networks, Ad hoc Networking, Routing Protocol.

1. Introduction

Mobile Ad-hoc Network is a collection of the mobile nodes that is formed without the support of any existing network infrastructure. The MANET is self configurable network, in which nodes connect and disconnect from the other nodes in the network automatically at any point of time. The characteristics of the MANETs are flexibility, distributed operation, addressing mobility, node to node connectivity, etc. Routing of the data in the MANETs are done on the basis of the node discovery i.e. the node receive the data and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination. Each node work as a relay agent to route the data traffic. As MANET is dynamic in nature so it is accessible to all the users it may be a legitimate user or the malicious node which reproduce the data or attack in the network.

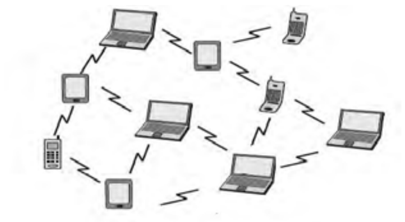

Figure 1:.Mobile Adhoc Network

1.1 Characteristics of MANET

1. No Centralized Administration – Each node in the MANET has its own communication capabilities for forwarding the data traffic over the network and adjusts according the topology.
2. Flexibility- MANET enables fast organization of the ad hoc network. When a node is to be associated with the network it should have the limited wireless communication range i.e. such node which can be available nearby.
3. Peer to peer connectivity of the nodes- In MANET the nodes neighbor to each other forms a set for communication to which request response messages are flooded.
4. Resource constraints- The node may have limited energy so this may limit the functionality of the network.
5. Dynamic Network topology-A node discovers the service of a nearby node using the service discovery protocol.
6. Heterogeneous Nodes – In the MANET architecture any node can participate in forwarding thee data packets, the node can be PCs, smart phones, smart tablets, embedded systems.

1.2 Applications

As Mobile adhoc network is infrastructure less and dynamic network so it is gaining popularity. Adhoc networks can be established anywhere where the nodes have connectivity with other nodes and can join and leave the network at any point of time. The applications of the MANET are as followed:-

- **Military:** -Using the adhoc network the communication among the soldiers, vehicles, and headquarters of military can be possible as this area do not have the proper establishment of the base station for the communication.
- **Emergency Services: -** Ad hoc can be used in emergency operations such as, search and rescue, recovery from disasters like fire, flood, volcano eruption, earthquake, etc. Information is relayed from one rescue team member to another over a small portable device.
- **Commercial environments: -**Ad hoc networks can autonomously link an instant in business so as to share the daily updates of office, in vehicular management to manage road traffic and accidents, inter-vehicle communication.

2. Classification of Routing Algorithms

1. On Demand Routing or Reactive Routing algorithms – In this category the protocols flood packets for the route

request in the network .The following protocols are in this category:-

- DSR (Dynamic Source Routing) Protocol-Each node maintains the route to the sink node during the packet transfer. For this DSR initiates the route discovery and route maintenance process. It flood route request (RREQ) packets and when packet reaches destination, a route reply (RREP) is generated.
- Ad-hoc On Demand Distance Vector (AODV) protocol-It maintain only active routes in the routing table for a pre-specified expiration time .Instead of flooding the RREQ, it maintains routing information of the active routes at each node.

2. Table driven routing algorithms or Proactive algorithm -In these protocols the nodes periodically exchange the routing information among the existing nodes so as to keep in turn information up to date.

- Optimized Link State Routing (OLSR) Algorithm uses two types of messages HELLO message and Topology Change TC message to discover and disseminate link state information throughout the nodes in the network

3. Hybrid Routing Protocol based on both the proactive and reactive approach.

- Zone Routing Protocol (ZRP) defines a zone around each node consisting of the node's *k*-neighborhood. If the source and sink of a packet are in the same zone, the packet is delivered immediately otherwise the route discovery happens proactively. The node forwards a route request message to the nodes which are at border of its zone.
- Temporally ordered Routing Algorithm (TORA)-It reacts to the change and link reversals. This protocol discovers the network portions showing link reversals and thus can stop the non productive links. It does not use HELLO message, in place of that it uses three phases route creation, route maintenance and productive route reversal.

3. Security Issues

Security in MANET is a major issue as to provide secure communication between the nodes in the infrastructure less environment. As adhoc network is self organizing, open node to node connections, dynamic topology, and limited resources. A secure network is that which possess the following attribute:

1. Confidentiality- To keep the information secret from the unwanted access. It is necessary to maintain the information safe and secure from the attacks.
2. Integrity of Message – To keep the accuracy and consistency of the data during its transit from node to node. So that the data is not modified by the unwanted access.
3. Availability of Nodes –As in MANET for communication the nodes are needed to be available all the time so that the information can be relayed over such path.
4. Authorization –it specify the privileges and the permissions of the entity participating in the communication over network.

4. Attacks in MANET

The network consists of heterogeneous nodes which can be a malicious node, whose intention is to attack the network and reproduce the false information. The attack can be classified as an active attack or passive attack.

Active Attack: In this the intruder attempts to break into the system, insert infected code, or steal information, destroy or reproduce it, thus disrupting the normal functionality of the network. It is classified into external attack and internal attack. The nodes which are not the part of network and attack on the data such type of attack is categorized as external attack while in the internal attack, the malicious node is an entity of internal network that propagates the false information.

Passive attack analyze network traffic i.e. identify the communicating entities, monitors message exchange between them ,decrypt weakly encrypted data, capture authentic data such as passwords, public key ,private key, that is exchanged over the link. From these messages, the inferences are drawn by the attackers regarding the messages and thus steal the information without the client or user information.

Table 1: Classification of Attacks in MANET

MANET Layers	*Types of Attacks*
Application Layer	Repudiation Data Corruption
Transport Layer	SYN flooding Session Hijacking
Network Layer	Black hole, Wormhole IP Spoofing Fabrication Modification
MAC Layer	Jamming

5. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to intercept. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node indicate the route availability as reply to the route request messages and thus capture the data packet and retain it. In protocol which is based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address

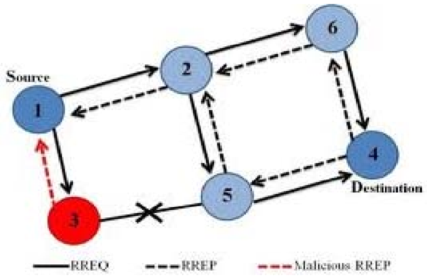

Figure 2: Black hole attack

Black hole in the AODV Protocol- The attacker can send a fake RREP to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and the attacker can misuse or discard the traffic.

Black hole in OLSR Protocol- An intruder node sends fake HELLO messages claiming it has links to more neighboring nodes than it actually have. Thus, there is a high probability that this node is chosen as an MPR (Multipoint relay) by its neighbor. The more neighbors the attacking node claims to have, the larger the potential impact of the attack on network. Due to the false messages sent by the attacker, in its neighborhood incorrect TC messages with too few entries or no TC messages due to an empty MPR selector set are propagated. Thus, the attacker is able to capture routes.

6. Detection and Removal Methods of Black Hole

WatchDog Scheme- Patcha et al [5] proposed a method for black hole attack prevention. A watchdog method is introduced in the network to tackle collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is elected should observe the neighboring node and decide whether it is a trusted node or a malicious node.

Neighborhood-based and Routing Recovery Scheme Sun et al [6] gave a general approach for the detection of the black hole attack. The method given by them is neighbor based, which detect the malicious node and a routing recovery protocol to establish a correct path to the truthful destination. For this such nodes which within the transmission range of a node forms neighboring node set. The control packets are used to share neighbor set with the other nodes. If two set received at same time and contains different elements, concludes the set generation by two different nodes.

Signature Algorithm - Gao et al [7] projected a signature algorithm to trace packet dropping nodes. The proposal consisted of algorithms to create proof, checkup algorithm and diagnosis algorithm

Time-based Threshold Detection Scheme [8] Latha Tamilselvan et al. propose a solution based a timer approach. A timer is started when first request is received and remain active while the other request from other nodes are collected. It will store the packet’s sequence number and received time and count the timeout value based on arriving time of first route request and analyzes the route belong to valid or not based on the threshold value.

Intrusion Detection System based on Anti-black hole mechanism [9] Ming-Yang Su proposes an IDS scheme to remove the black hole attacks in MANET The ABM employs two tables called RQ table and SN table The IDS work on the irregular difference between routing information transmitted from a suspicious node. If the value goes beyond the threshold value. It is considered as black hole. A block message is broadcasted by IDS system to all nodes .The block table which is maintained by all nodes add up this malicious node also. Whenever the route is established this block table is checked and no route reply message will be received from such nodes.

Resource-Efficient Accountability (REAct) Scheme based on Random Audits [10] William Kozma Jr. et al. presented a scheme for detection of the misbehave node. The REAct is triggered automatically when the performance statistics which depend on throughput, packet delivery rate etc. is descended between the sending node and a destined node. The solution consists of three phases (a) the audit phase (b) the search phase and (c) the identification phase. The target of destined node sends a feedback to the sender when a large packet drop ratio is identified. Then the source node selects an audit node, and to produce a behavioral proof against the node which is dropping the packets. Such nodes are identified and no further route reply messages are accepted from them.

Hash based Scheme [11] Weichao Wang et al. design a hash based method to produce node behavioral proofs which contain the data traffic information within the routing path .The scheme is based on auditing technique for prevention of the packet drop attack. The audited node ni is needed and settled by the source node which sends the sequence numbers of selected packets to auditing node. After source node sends out these packets, an additional random number t0 is attached to every packet. The intermediate node n1 combines the received packet and its own random number r1 to calculate its value t1, and this operation is continued within every intermediate node until ni receives the packet.

Bait DSR (BDSR) based on Hybrid Routing Scheme [12] Po-Chun Tsou et al. design a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol.

In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and non-existent. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. Therefore the source node can recognize the location of attacker from the reply location of RREP. All of the response sent by the adversaries should be drop. If the data delivery rate is lower than the pre-defined threshold value, the bait procedure will be triggered again to examine the uncertainly suspicious nodes.

References

[1] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao ; A survey of black hole attacks in wireless mobile ad hoc networks ; Human-centric Computing and Information Sciences 2011

[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester; An Overview of Mobile Ad Hoc Networks: Applications and Challenges

[3] Siddhu Warrier ; report on Characterization and Applications of MANET Routing Algorithms in Wireless Sensor Networks

[4] Masahiro Hiyama, Elis Kulla, Tetsuya Oda, Makoto Ikeda and Leonard Barolli; Application of a MANET Testbed for horizontal and vertical scenarios performance evaluation using delay and jitter metrics.

[5] Patcha; A. Mishra; Collaborative security architecture for black hole attack prevention in mobile ad hoc networks; Radio and Wireless Conference, 2003, 75-78.

[6] Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black-hole Attack in Mobile Ad Hoc Networks

[7] X.P. Gao; W. Chen; A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks; IFIP International Conference on Network and Parallel Computing Workshops, 2007

[8] Tamilselvan L, Sankaranarayanan V (2007) Prevention of Blackhole Attack in MANET. Wireless Broadband and Ultra Wideband Communications, Sydney, Australia

[9] Su M-Y (2011) Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications

[10] Kozma W, Lazos L (2009) REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits.

[11] Wang W, Bhargava B, Linderman M (2009) Defending against Collaborative Packet Drop Attacks on MANET

[12] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L (2011) Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs.

Author Profile

Ms. Swati Jain, M. Tech Scholar, Suresh Gyan Vihar University, Jaipur pursuing M. Tech in Computer Science and Engineering .She completed her Bachelor of Engineering degree in CSE in the year 2009 from Rajasthan University and Polytechnic Diploma (CSE) in year 2006 from Board of Technical Education, Rajasthan .Her research interest includes Computer Network, Wireless Sensor Networks.

Prof. (Dr.) Naveen Hemrajani, Principal (Engg.),SGVU and Chairman CSI (Jaipur Chapter) received his B.E degree in Computer Science & Engineering from Shivaji University in the year 1992 and M.Tech(CSE) in 2004. His Research Topic for PhD was Admission Control for Video Transmission over IP Networks. He possesses 21 years of Teaching and research experience. He has published three books and many research papers in International and National Journals of repute. He has also presented several papers in International and National conferences. He is also Editorial Board member of many international Journals of repute. He is also working on AICTE and DST (Department of Science & Tech.) sanctioned projects.