A SURVEY OF ROUTING PROTOCOLS AND WORMHOLE ATTACK IN MOBILE AD HOC NETWORKS

Deepika Arora*

Sweety Goyal**

ABSTRACT

A mobile ad hoc network is a set of wireless devices called wireless nodes which are dynamically connected by wireless links. Because of its characteristics of self configuration, wireless medium and absence of any established infrastructure, it is easy to set up and thus has become attractive to users. Security has been the primary concern in MANETs so as to provide the protected communication between the wireless nodes. The open and dynamic environment of MANET makes it vulnerable to various security attacks. One of the severe attacks on routing protocols in MANETs is the wormhole attack. In wormhole attack, two or more attackers connect to each other via a link called as tunnel or wormhole link which is a private high speed network. This attack in MANET is quite challenging to defend against. In this paper, we will discuss some basic routing protocols like DSDV, OLSR, WRP, DSR and AODV. Also we examine the wormhole attack in existing MANET protocols.

*Lecturer, Department of Computer Science & Engineering, Maharishi Markandeshwar Engineering College, MMU, Mullana, Ambala, Haryana.

**Lecturer, Department of Information & Technology, Maharishi Markandeshwar Engineering College, MMU, Mullana, Ambala, Haryana.

I. INTRODUCTION

Mobile Ad hoc Network is a set of wireless devices called wireless nodes or mobile nodes that dynamically connect and transfer information. Mobile ad hoc network does not have any centralized coordinator or any infrastructure because of which security in such networks is of primary concern.

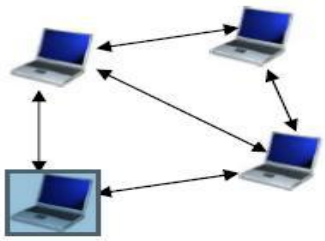

Fig 1: Routing in MANET

These networks does not have a fixed topology, here nodes can act both as host as well as routers. A wireless node can be the source, the destination or any intermediate node of data transmission. The routing protocols in MANET come under two major categories: proactive routing protocols and reactive routing protocols.

In this paper, section II gives you the brief working of various routing protocols like DSDV, WRP, OLSR, DSR and AODV. Section III describes the various attacks on routing in MANET. After that, an overview of wormhole is given in section IV. In section V we conclude the paper.

II. ROUTING PROTOCOLS

In a mobile ad hoc network, it may be necessary to hop several hops (multi-hop) before a packet reaches the destination, a routing protocol is needed. The routing protocols have two main functions, selection of routes and delivery of messages to their correct destination.

Two major categories fall for routing protocols in MANETs as proactive routing protocols also called as table driven routing protocols which attempt to maintain consistent, updated routing information from one node to every other node. Some of these protocols are: DSDV, OLSR, CGSR and WRP. The second category includes the reactive routing protocols also known as on demand routing protocols that invoke a route determination procedure on demand only. AODV, DSR and TORA are reactive protocols.

A. DSDV (Destination Sequenced Distance Vector)

The destination sequenced distance vector routing protocol is a table driven routing protocol, where each node in the network maintains a routing table which includes the number of hops required to reach the destination node and the neighboring node in the path. The routing table

consists of a sequence number generated by the destination node which enables the mobile node to ensure the freshness of the route which further avoids the formation of any routing loops. [2]

DSDV guarantees loop free routes through the use of sequence numbers. When a node receives new information that involves an already active route, the node compares the sequence number of the update and the existing routes in the table. If the new sequence number is greater than the one in the table, the entry for that route is modified. Otherwise, the update is discarded and no modification is made.

B. OLSR (Optimized Link State Routing)

The optimized link state routing protocol is a proactive routing protocol. In OLSR, nodes must transmit periodic topology information. OLSR introduces the concept of multipoint relay (MPR) nodes. The main purpose of MPR nodes is to allow an optimal transmission of LSAs (Link State Advertisement) which provides an efficient flooding mechanism. Each node in the network must choose a minimal set of MPRs from its 1-hop neighbors. For a node, its MPR set is the set of its neighbors that are at most two hops away from itself. [6]

We have two types of routing messages in OLSR routing protocol, named as HELLO messages and Topology Control (TC) messages. The hello messages generated by a node allows the nodes to know about their neighbors are exchanged t a fixed interval of time. The node's HELLO message contains the node's own address and a list of neighbors. The topology control (TC) messages are used for calculating the routes and are exchanged by nodes to get to know the topology information. Only MPR nodes can forward the TC messages. Upon receiving TC message from fellow nodes, a node can create new entries or can modify the old entries of routing table [5].

C. WRP (Wireless Routing Protocol)

Wireless routing protocol is also a table driven routing protocol which guarantees the loop freedom and avoids the routing loops by using the predecessor information. Each node has to maintain four routing tables; distance table, routing table, link cost table and message retransmission list table [2]. This introduces a memory overhead at each node as the network size increases. Each node is forced to check predecessor information, WRP avoids count-to-infinity problem.

D. DSR (Dynamic Source Routing)

Dynamic source routing [1] is a reactive routing protocol which is source initiating routing protocol rather than table based. In DSR, each packet needs to carry the full address from source to the destination. This protocol consists of two main methods*:* route discovery and

route maintenance. This protocol involves route caching, where every node maintains a cache which stores recently discovered paths.

Whenever a node has the packet to send to the destination, the source node check its route cache for a valid route before initiating route discovery and if a valid route is found there is no need for route discovery, it will use this route to send the packet. If it does not have a valid route to the destination, the source node initiates route discovery process and sends a route request packet by broadcasting it to neighbors. A node upon receiving route request packet, checks their routing cache for a route to the destination if it finds the route, a route reply message is sent back to the source node. If no such route is found, node rebroadcasts the route request packets to its neighboring nodes. When the route is discovered, the packets will be transmitted by the source node on the route discovered.

Route maintenance phase in DSR monitors the correct operation of route. The route maintenance may be provided by using either hop-to-hop or by end-to-end acknowledgements, in case of hop-to-hop acknowledgements, the hop in error is indicated in the route error packet. Any host if detects that its neighboring node, which is the next hop is not working then the node send an error packet containing its address and the address of the hop not working. A node upon receiving the route error packet removes the hop in error from its routing cache. In case of end to end acknowledgements the source node assumes that the last hop of the route to the destination is error.

E. AODV (Ad hoc On Demand Distance Vector)

Ad hoc on demand distance vector protocol is a reactive protocol that reacts on demand and is based on DSR and DSDV [3]. It uses the sequence numbering procedure of DSDV and a similar route discovery procedure in DSR. This protocol creates routes purely on demand basis, which reduces the number of required broadcasts. AODV is a loop free routing protocol because of the concept of sequence numbering which it has got from DSDV. When a source node has the data packets to send to the destination, it initiates a route discovery process by broadcasting the RREQ packet to its neighbors. The neighbors who receive RREQ, rebroadcasts these RREQ to their neighbors and this process continues until it reaches the destination node. The destination node then sends back the RREP packet to the source following the reverse path.

III. SECURITY ATTACK ON MANET

There can be various possible ways in which malicious node(s) can attack in MANET. These can be generating invalid routing information, sending invalid messages to a node several

times. Also a malicious node can advertise invalid links to disrupt the routing in MANET. Such attacks can be broadly classified in two categories: Active Attacks & Passive Attacks.

Let us discuss some of the most common attacks that cause a big security concern in MANET.

a) Impersonation

A malicious node can launch many attacks in a network by masquerading as another node (Spoofing). Spoofing occurs when a malicious node misrepresents its identity and the traffic that belongs to the impersonated node is redirected to the malicious node.

b) Modification

A malicious node may attack by altering the protocol fields of messages passed among the nodes. Malicious node can easily cause traffic subversion and denial of service by setting the false values of various fields in the packet such as route sequence numbers.

c) Fabrication

In such type of attack, an attacker or malicious node generates the false routing information. Because the routing constructs comes as valid so such kind of attacks are difficult to indentify. For example, a false RERR route error message can be generated by an attacker, which claims that a neighbor can no longer be contacted.

d) Wormhole Attack

In this type of attack, two colluding malicious nodes create a tunnel between them using a private high speed network(s). This attack allows a node to short-circuit the normal flow of routing message. The attacker at one end collects the data and replays them at the other end using tunnel.

e) Blackhole Attack

An intruder can launch this attack by sending false routing information and advertise itself as having an optimum path to the destination node. For example, a malicious node can reply for route request falsely without having an active route to the destination and causes other good nodes to route data packets through the malicious node.

IV. WORMHOLE ATTACK AND VARIANTS

Wormhole attack is a kind of replay attack which is very hard to defend against. It is such an attack which cannot be detected using any of the cryptographic solutions. A wormhole consists of two malicious nodes and a high bandwidth link, which is called as wormhole tunnel. In this attack, an intruder at one end of the tunnel records the packet and at the other end replays them using wormhole tunnel.

A wormhole attack [9] in wireless network can be launched by four ways:

a) **Packet encapsulation**

In this mode, encapsulated packets are sent between two malicious nodes. Here one malicious node encapsulates the packet and sends it to the other malicious node and hop count does not get increased with this traversal.

b) **Out of band**

In this mode, the malicious nodes use a high bandwidth channel between them.

c) **High power transmission**

In this mode, the malicious node broadcasts the RREQ packet with high power level. The other node in the network does not have such a power. The node that hears such a high power broadcast must be a malicious node and rebroadcasts it to the destination.

d) **Packet relay**

In this mode, the malicious node relays data packets between two nodes that are far apart and convince them they are neighbors.

V. CONCLUSION

MANET has become a very hot research topic these days as MANET is an infrastructure less network having no centralized coordinator. Because of this MANET are vulnerable to many attacks. In this paper, we have reviewed about various routing protocols and wormhole attack in MANET.

VI. REFERENCES

1. Sunil Taneja, Ashwani Kush, "A Survey of Routing protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, ISSN: 2010-0248, August 2010.
2. Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, volume (2) issue (3).
3. Jatin D. Parmar, Ashish D. Patel, Rutvij H. Jhaveri1, Bhavin I. Shah, " MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.
4. Reshmi Maulik, Nabendu Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3, pp. 271-279, 2011.

5. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE, pp. 1536-1284, October 2007.
6. Abari Bhattacharya, Prof. Himadri Nath Saha, "A Study of Secure Routing in MANET: various=attacks and their Countermeasures", IEMCON 2011 organised by IEM in collaboration with IEEE in Jan,2011.
7. Majid Meghdadi, Suat Ozdemir, Inan Guler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, Vol. 28, Issue 2, Mar-Apr 2011.
8. R. Maulik, N. Chaki, "A Comprehensive Review on Wormhole Attacks in MANET". In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications, pp. 233-238, 2010.
9. Pallavi Sharma, Prof. Aditya Trivedi, "An approach to defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", IEEE, 978-1-61284-486-2