An Analysis of MANETs: Types of Routing Protocols, Types of Attacks on Security

#1A Vanaja, #2Jeevan L. J. Pinto
#1 Research Scholar, Visvesvaraya Technological University, Belagavi, Karnataka, India
*2 Associate Professor, Department of Computer Science and Engineering,
Yenepoya Institute of Technology, Moodbidri, Karnataka, India

Abstract— **A Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes or terminals which communicate with each other by forming a multi-hop radio**
Network and maintaining connectivity in a decentralized manner over relatively bandwidth constrained wireless link. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. The topology is highly dynamic and frequent changes in the topology may be hard to predict. In this paper we discuss about various types of routing protocols and different type's security attacks in MANETs.

Keywords— ***MANET, Types of Routing Protocols, Various attacks of MANET.***

I. INTRODUCTION

Mobile Ad hoc network is a group of autonomous mobile nodes which can communicate to each other via radio waves. In Mobile ad hoc network each device has feature of dynamic move and form a decentralized network. So it leads to frequent changes in topology Which is a challenge to send the packets to the targeted nodes [1]. In an ad hoc network, a node can communicate with another node either unicast or broadcast depends on the current position of the node.

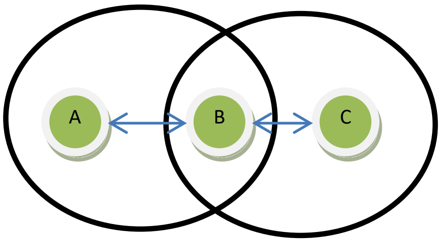

Figure 1: Mobile Ad-Hoc network

When a two communicating nodes are in the same transmission zone then it can communicate through unicast, while the communicating node is in another zone is carried out by broadcasting method [2]. The fundamental issue in ad hoc networking is routing i.e. how to deliver data packets among mobile nodes efficiently without predesigned topology or with decentralized control, which is the main objective of ad hoc routing protocols. Since mobile ad hoc networks change their topology very frequently, routing in such networks is a challenging task [1].

II. BROADCASTING APPROACHES IN MANET

In MANET [3], a number of broadcasting approaches on the basis of cardinality of destination set:

A. **Unicasting:** Sending a message from a source to a single destination.

B. **Multicasting**: Sending a message from a source to a set of destinations.

C. **Broadcasting**: Flooding of messages from a source to all other nodes in the specified network.

D. **Geocasting**: Sending a message from a source to all nodes inside a geographical region.

III. TYPES OF ROUTING PROTOCOLS

Routing is the most fundamental research issue in MANET and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable movements of nodes. Generally, current routing protocols for MANET can be categorized as:

- Routing information update mechanism
- Use of temporal information for routing
- Routing topology
- Utilization of specific resources

1) Based on routing information update mechanism:

In this approach a mobile node uses its knowledge about recent connectivity of the network including the state of network links[4]. Based on the route updating, routing protocols are classified into three categories.

a. Proactive Routing Protocol
b. Reactive Routing Protocol
c. Hybrid Routing Protocol

a) Proactive (Table – Driven)

In this approach the nodes maintain consistent, up-to-date routing information of the whole network[5,6]. Each node has to maintain one or more tables to store routing information, and response to changes in network topology by broadcasting and propagating. Some of the typical proactive routing protocols for MANET are Wireless Routing Protocol (WRP), Destination Sequence Distance Vector (DSDV) and Fisheye State Routing (FSR).

b) *Reactive (Source-Initiated On-Demand Driven)*

In this approach nodes are discovered only when they are actually needed. Whenever a node has data to send to some destination, first it checks its route table to know whether it has a route. If the route doesn't exist in table, then it will find a path to the destination. Hence, route discovery becomes on-demand. This approach is therefore also called as on-demand routing. Some of typical Reactive routing protocols for MANET are Dynamic Source Routing[5] protocol, Ad-hoc On-demand Distance Vector (AODV).

c) *Hybrid Protocols:*

Hybrid routing protocols [5, 7] the combination the proactive and reactive approaches. Cluster a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. . Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For nodes that are located beyond this zone, an on-demand approach is used. Zone Routing Protocol (ZRP)[8]is an example of hybrid routing protocol.

III. ROUTING ISSUES WITH MANET

The following are some of the main routing issues to be considered when deploying MANETs

- Unpredictability of Environment.
- Unreliability of Wireless Medium.
- Resource-Constrained Nodes.
- Dynamic Topology.
- Bandwidth-constrained.
- Limited physical security.
- Energy.
- Routing over head.

IV. VARIOUS TYPES OF ATTACKS IN MANET

In wireless ad-hoc networks security is a highly challenging issue[9,10]. Studying all possible aspect of attacks is always the primary step towards developing good security solutions. Security of communication in MANET is essential for secure transmission of information. MANET attacks can be broadly classified as various categories like internal attacks, External attacks, Active Attacks Passive Attacks. Attacker can harm the network as internal, external or active, passive so these classifications are very important.

1. **External Attack**: External attacks are carried out by third party nodes that who do not belong to the particular network and they try to halt the network by passing spoofed information. It causes the malfunctioning of network.
2. **Internal Attack**: Internal attacks are from the internal nodes that are part of the network. The attacker may be a new node that is added to the network , which may gain the access to a network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities. It is difficult to predict the internal attacks as compared to external attack.
3. **Passive Attack:**
In this attack, an attacker only listens and keeps track of information that is being communicated between two nodes. No modification is done on the message. Attackers can easily get all the information about the complete network that is useful in hijacking or injecting an attack in the network. It is difficult to detect passive attacks as compared to active attacks.
4. **Active Attack**

In this attack, an attacker listens and attempts to modify or alter the data being exchanged in the network. It may interrupt the normal functioning of the networks. In active attack, the intruders can modify the packets, inject the packets, drops the packets or it can use the various feature of the network to launch the attack.

5. **Wormhole Attack:** In a wormhole attack, an attacker trap and stores the packets at one location in the network and tunnels them to target point in the network, and then resend them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

6. **Denial of Service attack**: In this type of attack an sends huge amount of packets or unwanted traffic simultaneously to a server and trying to slow down the server due to which the resources will not be available to the user. The attacker generally uses radio signal jamming and the battery exhaustion method.
7. **Impersonation**: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.
8. **Routing Attacks:** The malicious node target the routing services as it is very important service in MANETs. There are two bite to this routing attack. One is attack on routing protocol and another one is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The second one is aimed at disturbing the packet delivery against a predefined path.
9. **Black hole Attack:**: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[9] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

10. Replay Attack: An attacker that performs a replay attacks are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

11. Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered. **12. Man- in- the- middle attack:** An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

13. Gray-hole attack: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

V. CONCULSIONS

This paper presents a complete study of various types of MANET protocols and the various issues. In addition, we also focused the different MANETs attacks for some security issues like internal attacks, External attacks, Active Attacks Passive Attacks.

REFERENCES

[1] Rajeev Kumar ,Kailash Patidar , Megha Jain, “A Survey on Routing Protocols with Performance Parameters for Different Number of Nodes” Journal of Network Communications and Emerging Technologies (JNCET) , Volume 6, Issue 2, February (2016)

[2] Brad Williams, Tracy Camp “Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks “MOBIHOC’02, June 9-11, 2002, EPFL, Lausanne, Switzerland. 2002 ACM 1-58113

[3] IIyas, M., 2003. The hand book of ad -hoc wireless networks. CRC press LLC

[4] Priyanka Goyal, Vinti Parmar, Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application” IJCEM vol 11, January 2011, ISSN(Online):2230-7893.

[5] Belding-Royer,E.M. and C.K. Toh, 1999. A review of current routing protocols for ad-hoc mobile wireless networks.IEEE Personal Communication magazine pp:46- 55.

[6] E. M. Royer and C-K Toh , ―A review of Current routing protocols for Ad Hoc Mobile Wireless.

[7] M. Frodigh, P. Johansson, and P. Larsson.―Wireless ad hoc networking: the art of networking without a network,‖ Ericsson Review,No.4, 2000, pp. 248-263.

[8] Rabia Ali, Fareeha Zafar, “Bandwidth Estimation in Mobile Ad-hoc Network” IJCSI , Vol 8, Issue 5, ISSN(online):1694-0814.

[9] K Rajkumar, s.Prasanna “Complete analysis of various attacks in MANET”, IJPAM Volume 119 No. 15 2018, 1721-1727, ISSN: 1314-3395 (on-line version)

[10] M.Bheemalingaiah, M.M Naidu,” Survey of Routing Protocols, Simulation Tools and Mobility Models in Mobile Ad Hoc Networks”, IJIACS ISSN 2347 – 8616 Volume 6, Issue 11 November 2017