Mitigating Routing behavior in Mobile wireless network with various types of routing attacks

M Jhansi
Assistant Professor, Department of Computer Science & Engineering,
MLR Institute of Technology, Hyderabad, Telangana, India

Dr M Bal Raju
Principal, Krishna Murthy Institute of Technology and Science
Hyderabad, Telangana, India.

B Raswitha
Assistant Professor, Department of Information Technology,
MLR Institute of Technology, Hyderabad, Telangana, India

Abstract- A MANET is a Versatile Ad Hoc Network framework is a self organized network consisting of mobile nodes can freely move in a wireless communication environment. The main purpose of an ad hoc network routing protocol is to enable the transport of data packets from one point to another. Security is an important issue if we look at mobile in a multi hop environment. The idea of ad-hoc networks have created a lot of interest in the research community, and it is now starting to materialize in practice in various forms, ranging from static sensor networks through opportunistic interactions between personal communication devices to vehicular networks with increased mobility. This paper provides a qualitative analysis of how proactive and reactive protocols cope with malicious internal attacks, and whether one type of protocol offers inherently better resistance to the various attacks.

Keywords – MANET, Routing, Attacks.

I. INTRODUCTION

In Wireless Adhoc environment nodes present in the network moves around the whole network during this process we may expect that the malicious node acting as a misleading node sends the fake messages may times, we call this behavior as an attack in routing. In Network layer two main operations are performed in MANET one is Adhoc routing another one is Data packet forwarding, the layer which provides mobile nodes one hop connectivity using Link Layer Protocol and different multi hop using Network Layer Protocols, which can be used to provide coordination among nodes by assuming all mobile nodes in wireless environment are cooperative using the technique call Reputation Based Method. Because of the presence of malicious attackers that violates the protocol specification in order to disrupt the network operations.

II. EXISTING METHODS FOR DETECTING ROUTING ATTACKS

Attacks can be detected in Manet in various ways if we look at the Profile-based detection method always it is based on behavior detection. It defines a profile of normal behavior and classifies any deviation of that profile as an anomaly. The assumption of this type of detection is that attacks are events distinguishable from normal legitimate use of system resources. Although, this type of anomaly detectors are able to detect novel attacks they are prune to high false positive rate due to the difficulty of clear segmentation between normal and abnormal activities and the use of insufficient or inadequate features to profile normal behaviors. The same way Specification-based detection method defines a set of constraints that describe the correct operation of a program or protocol and monitors the execution of the program with respect to the defined constraints. It has been show that specification-based techniques live up to their promise of detecting known as well as unknown attacks while maintaining a very low rate of false positives. Since, the increasing popularity of wireless networks to that of wired networks, security is being considered as a major threat in them. Wireless network exposes a risk that an unauthorized user can exploit and severely compromise the network. There can be different possible attacks in wireless network viz., active and passive attacks. So there is a need for secured wireless system to analyze and detect number of attacks

III. ROUTING PROTOCOLS BEHAVIOR

3.1 Proactive Protocol and Reactive Protocol Context

According to the context of DSR [1] MANET routing protocol there are different attacks an attacker modifies source routing list with respect to RREQ or RREP packets. Switching order of different nodes in the routing list. Deleting entries from the list. Appending new node entries into the list. According to the context of AODV [2] MANET routing protocol there are different attacks which an attacker advertise route with wrong distance metric with respect to actual distance to the destination. Advertise wrong routing updates with a large sequence number with respect to actual sequence number. An attacker invalidates all routing updates from other nodes. According to the context of TORA routing protocol, there are also different attacking methods that Attackers construct routing paths by interfering with the protocols' mechanisms, e.g. routes can be forced to use attacking nodes to go through them. Attackers can also exhaust network resources by maliciously act of injecting, modifying and dropping data packets.

Generally there are four different types of MANET routing protocol attacks which is divided in to two main types which are given below:

1. Routing disruption attacks
2. Resource consumption attacks

In case of routing disruption attacks, the main task of attacker is to disrupt routing process by routing packets in order to introduce wrong paths. In case of resource consumption attacks are concerned the main task of the attacker is to introduce some non-cooperative or selfish nodes that can which are given below.

be used to inject false packets due to this way load on the network increases and it will become a cause of consuming network bandwidth. Mainly both of these attacks in MANET routing protocols are the best examples of Denial of Service (DoS) attacks. In Figure 1 there is a broader classification attacks in MANET routing protocols.

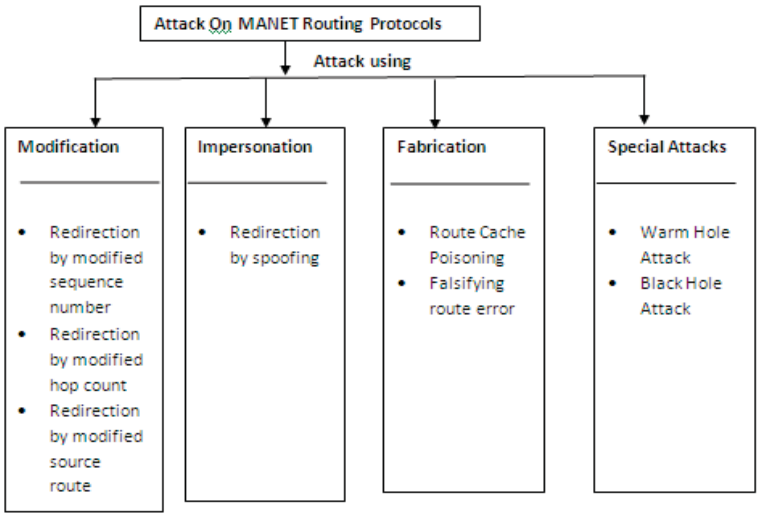

Fig 1: Classification of Attacks in MANET Routing Protocols

3.2 Attacks Using Modification

This types of attacks send some of the messages in the protocol fields are modified and then these messages passed among the nodes, due to this way it become the cause of traffic subversion, as well as traffic redirection and also act as a Denial of Service (DoS) attacks.

3.2.1 Route Sequence Numbers Modification

This types of attacks mainly possible against the AODV protocol. In this case an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

3.2.2 Hop Count Modification Attack

This types of attacks where it is also mainly possible against the routing protocol AODV, here attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

3.2.3 Source Route Modification Attack

This types of attacks which is possible against DSR routing protocol where attacker (malicious node) modify source address and move traffic towards its own destination.

3.3 Attacks Using Impersonation

This types of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other user node in order to change the network topology. This type of attack can be described in the Figure 2 given below:

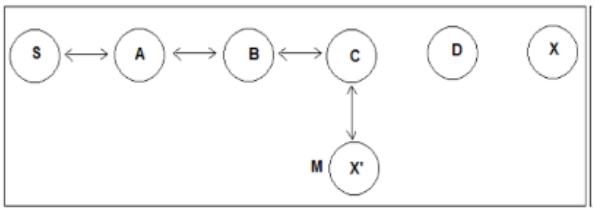

Fig 2: Impersonation Attack

In the above figure where the S node wants to send data towards the node X and before sending data to node X it starts a Route Discovery process. During route discovery process there is a malicious node M, when it receive route discovery packet regarding the node X then it modify its address and change to node X, like impersonates node X as X'. After that it send packet back to source node S that I am the destination node by RREP packet request. When the source node receives RREP packet information it doesn't authenticate node and accept the route and send data to the malicious node. This type of attacks also called routing loop attack which will become the cause of loops within the network.

3.4 Attacks Using Fabrication

This types of attacks where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network. Attacks using fabrication process are discussed very well in [20] and [21]. In Figure 3. Where fabrication attacks is explained by an example. In the example where the source node S wants to send data towards the destination node X, so therefore at start it sends broadcast message and request for route towards the destination node X. An attacker as a malicious node M try to pretends and modify route and returns route reply to the node (S). Furthermore, an attacker's nodes use to fabricate RERR requests and advertise a link break nodes in a mobile ad hoc network by using AODV or DSR routing protocols.

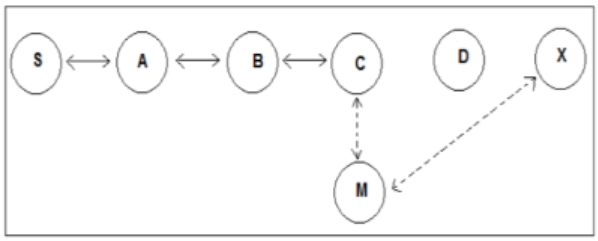

Fig3:Fabrication Attack

3.5 Special Attacks

There are also some other severe attacks in MANET network which are possible against routing protocols such as AODV and DSR

3.5.1 Worm Hole Attack

This types of attack one of the severe types of attack in which an attacker introduces two malicious nodes in the network where an attacker used to forward packets through a private "tunnel". The scenario is shown in the below Fig 4.

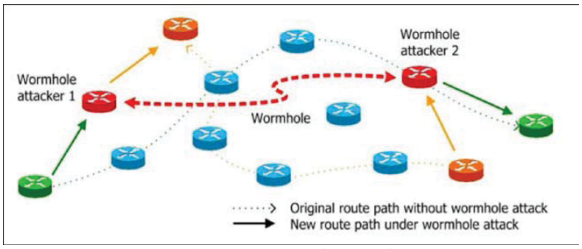

Fig4: Warm Hole Attack

3.5.2 Black Hole Attack

This type of attack is described very well in detail in [21]. In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property. The scenario is shown in the below Fig 4.

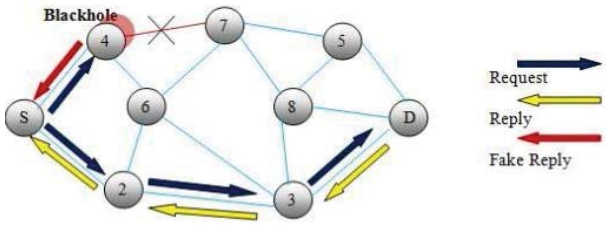

Fig5: Black Hole Attack

IV.TYPES OF ACTIVE ATTACKS ON VARIOUS LAYERS IN PROTOCOL STACK

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack.

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Blackhole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Eavesdropping, jamming, active interference

V.SECURITY GOALS

The goal of system security is to have controlled access to resources. The key requirements for networks are confidentiality, authentication, integrity, non repudiation, and availability

Confidentiality: it protects data or a field in message. It is also required to prevent an adversary from traffic analysis.
Integrity: it ensures that during transmission the packets are not altered.
Authorization: it authorizes another node to update information or to receive information.
Availability: it ensures that services are available whenever required.
Resilience to attacks: it is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.
Freshness: it ensures that malicious node does not resend previously captured packets.
Anonymity: this service helps for data confidentiality and privacy.
Access control: it prevents unauthorized access to a resource.

VI.CONCLUSION

Nowadays everyone has laptops, Smartphone's, PDA's and they want to connect these devices with others device so that they can exchange information and MANET is the only solution to it. It is temporary network which is set up on the temporary basis and disconnected when the work has been done. It is better for small area only. It has great applications in the field of military, hospitals (fast retrieval of data), education (virtual classrooms, conferences), emergency (disaster, earthquake). Sensors are small device that are deployed in a particular are for sensing the data or information. Micro sensors are used in military, health industries, food industries, used for environmental and weather information gathering. But it is also true that this network is vulnerable to several attacks i.e. security is the major issue in wireless network. Hence this paper shows different types of attacks in MANET. This paper focused on active attacks like black hole, Wormhole, Sleep deprivation Torture attack, Sybil attack etc. And some of the detection techniques are also described to prevent these attacks.

REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.
[2] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.
[3] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.
[4] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park
[5] K.P. Manikandan, Dr. R .Satyaprasad, Dr. Rajasekhararao. "Analysis and Diminution of Security Attacks on Mobile Ad hoc Network".IJCA Special Issue on "Mobile Ad-hoc Networks "MANETs, 2010