A Survey of Routing Attacks in Manet

R.LATHA

M.Phil Research Scholar -Computer Science,SreeSaraswathiThyagarajaCollege,Pollachi

Mail Id: lathacs33@gmail.com

S.SASIKALA

Head of Department, Department of Computer Science,SreeSaraswathiThyagaraja College, Pollachi

----------**ABSTRACT**----------

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined organization of available links, which makes any node in the network act as a potential router.The nodes dynamically establish paths among one another.Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks like worm whole, black hole, rushing attack etc. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. This flexibility, along with their self-organizing capabilities, are some of MANET's biggest strengths, as well as their biggest security weaknesses.

Keywords: Manet, dynamic topology, vulnerable, Security attacks, wormhole.

---

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with
each other hop by hop following a set of rules (routing protocol) for the hopping
Sequence to be followed. The chief characteristics and challenges of the MANETs can be classified as follows:

1.1Dynamism of Topology

The nodes of MANET are randomly, frequently and unpredictably mobile within the network. These nodes may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity ofrouting. Suchmobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes
1.2 Lack of fixed infrastructure

The absence of a fixed or central infrastructure is a key feature of MANETs. This eliminates the possibility to establish a centralized authority to control the network Characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

1.3 Resource constraints

MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring.

1.4 Cooperation

If the source node and destination node are out of range with each other than the communication
Between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes is formed. This is known as multi hop communication. Hence each node is to act as a host as well as a router simultaneously.

2. ROUTING PROTOCOLS IN MANETS

The nodes in MANETs perform the routing functions in addition to the inherent function of being the hosts. The limitation on wireless transmission range requires the routing in multiple hops. So the nodes depend on one another for transmission of packets from source nodes to destination nodes via the routing nodes. The nature of the networks places two fundamental requirements on the routing protocols. First, it has to be distributed. Secondly, since the topology changes are frequent, it should compute multiple, loop-free routes while keeping thecommunication overheads to a minimum. Based on route discovery time,
MANET routing protocols fall into three general categories

a) Proactive routing protocols
b) Reactive routing protocols
c) Hybrid routing protocols

2.1 Proactive Routing Protocols

In the proactive routing protocols, routing is done using the information present in routing tables maintained at each node i.e. table driven routing. These tables are exchanged on a periodic basis between the nodes. Each entry in the table contains the information of the next hop for reaching to a node or subnet and the cost of this route. Since information of the neighboring nodes is maintained at each node, the time for route selection becomes minimal.

2.2Reactive routing protocols

Reactive MANET protocols only find a route to the destination node when there is a need to send data. The source node will start by transmitting route requests throughout the network. The sender will then wait for the destination node or an intermediate node (that has a route to the destination) to respond with a list of intermediate nodes between the source and destination. This is known as the global flood search, which in turn brings about a significant delay before the packet can be transmitted. It also requires the transmission of a significant amount of control traffic. Thus, reactive MANET protocols are most suited for networks with high node mobility or where the nodes transmit data infrequently

2.3Hybrid Routing Protocol

Hybrid protocol is presented to overcome the shortcomings of both proactive and reactive routing protocols. Hybrid routing protocol is combination of both proactive and reactive routing protocol. It uses the route discovery mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network. Hybrid protocol is suitable for large networks where large numbers of nodes are present. In this large network is divided into set of zones where routing inside the zone is performed byusing reactive approach and outside the zone routing is done using reactive approach.

3. ROUTING ATTACKS IN MANETS

All of the routing protocols in MANETs depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic assumption in such a setup is that all nodes are well behaving and trust worthy. Albeit in an event where one or more of the nodes turn malicious, security attacks can be launched which may disrupt routing operations or create a DOS (Denial of Service) condition in the network. Due to dynamic, distributed infrastructure-less nature of MANETs, and lack of centralizedauthority, the ad hoc networks are vulnerable to various kinds of attacks. The challenges to be faced by MANETs are over and above to those to be faced by the traditional wireless networks. The accessibility of the wireless channel to both the genuine user and Attackers make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers

The limited power backup and limited computational capability of the individual nodes hinders the implementation of complex security algorithms and key exchange mechanisms. There is always a possibility of a genuine trusted node to be compromised by the attackers and subsequently used to launch attacks on the network. Node mobility makes the network topology dynamic forcing frequent Networking reconfiguration which creates more chances for attacks.The attacks on MANETs can be categorized as active or passive.

Passive Attacks

In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non-disruptive but are information seeking, which may be critical in the operation of a protocol. Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network. A passive attacker listens to the channel and packets containing secret information (e.g., IP addresses, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. In a wireless environment it is normally impossible to detect this attack, as it does not produce any new traffic in the network.

Active Attacks

Injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and non-repudiation paradigm. Contrary to the passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an ad hoc network.

The first approach to develop security solutions is the understanding of potential threats. Supported by this threat analysis and capabilities of potential attackers, the well-known routing attacks in MANETs are discussed.

3.1Flooding attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can

send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial of service.

3.2Sleep Deprivation

In sleep deprivation attack, the resources of the specific node/nodes of the network are consumed by constantly keeping them engaged in routing decisions. The attacker node continually requests for either existing or non-existing destinations, forcing the neighboring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.

3.3 Impersonation Attack

In impersonation attack attacker nodes impersonates itself as legitimate node and sends false routing information and masks itself as sending from trusted node.

3.4Black Hole Attack

In this attack, the attacker node injects false route replies to the route requests claiming to have the shortest path to the destination node whose packets it Wants to intercept. Once the fictitious route has been established the active route is routed through the attacker node. The attacker node is then in a position to misuse or discard any or all of the network traffic being routed through it

3.5Node Isolation Attack

The authors in this work have introduced an attack against the OLSR protocol. As implied by the name, the goal of this attack is to isolate a given node from communicating with other nodes in the network. The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes.

3.6 Routing Table Poisoning Attack

Routing Table Poisoning attacker corrupts the routing tables of other nodes in the networks resulting in the creation of false routes, suboptimal routes, formation of loops, and congestion in portions of the network and also in network partitioning.

3.7 Wormhole Attack

In wormhole attack involves the cooperation between two attacking nodes .One attacker captures the packet and tunnels it to the other attacker. The link between the attackers is high speed communication link. These two attackers make the topology under their Control

3.8 Location Disclosure Attack

In this attack, the privacy requirements of an ad hoc network are compromised. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, and the structure of the network.

3.9Rushing Attack

Rushing attacks are mainly against the on demand routing protocols. These types of attacks subvert the route discovery process. On demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react

3.10Blackmail

The attack happens due to lack of authenticity and it grants provision for any node to corrupt other node's legitimate information. Nodes usually keep information of perceived malicious nodes in a blacklist. This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and tell other nodes in the network to add that node to their blacklists and isolate legitimate nodes from the network.

3.11 Snare Attack

The snare attack, which relates to military specific applications. In a battlefield, a node could be physically compromised (say when the corresponding soldier is caught by the enemy). Afterwards, the compromised node could be used to lure a Very Important Node, (say the commander), into communicating with it. Since the adversary can easily intercept any transmission in the network through the compromised node, the adversary can identify the physical location of the VIN by tracing and analyzing some routes. After locating the VINs, the adversary will be able to launch a Decapitation Strike on those VINs as a short cut to win the battle.

3.12 The Invisible Node Attack

The invisible node attack and proved it to be different from the existing attacks (man in the middle, masquerading, and wormhole) and established its uniqueness. They have defined it as in any protocol that depends on identification for any functionality, any node that effectively participates in that protocol without revealing its identity is an invisible node and the action and protocol impact is termed an INA. Discussing the effects of INA on different routing protocols, they have shown it to be an unsolvable attack so far

4. CONCLUSION

In this paper, we have analyzed the security threats an ad-hoc network faces and presented the security objective that need to be achieved. On one hand, the security sensitive applications of an ad -hoc networks require high degree of Security on the other hand, ad hoc network are inherently vulnerable to security attacks. The research on MANET

security is still in its early stage. The existing proposals are typically attack oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats.

5. REFERENCES

[1]C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008. George Aggelou, Mobile Ad Hoc Networks, McGraw-Hill, 2004. [3]

[2] S. Agrawal, S. Jain, and S. Sharma, *"A survey of Routing Attacks and Security Measures in Mobile AdHoc Networks,"* Journal of Computing, Volume 3, Issue 1, January 2011, ISSN 2151-9617.

[4] M.A. Shurman, S.M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, pp. 96-97, 200

[5] Gagandeep, Aashima, PawanKumar,*Analysisof Different Security Attacks in MANETs on Protocol Stack A-Review*,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 –8958, Volume-1, Issue-5, June2012.

[6] PriyankaGoyal,SahilBatra , Ajit Singh, *A Literature Review of Security Attack in Mobile Ad-hocNetworks*, International Journal of Computer Applications (0975 – 8887) Volume 9–No.12, November 2010

[7] I.Chlamtac, M.Conti, and J.Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, vol. 1, no. 1, pp. 13-64, 2003.