Attacks in MANET

Dr Sanjeev Yadav
Director
LIET, Chikani,Alwar-Rajasthan

Rachna Jain
Assistant Professor
Amity University, Noida

Mohd Faisal
Assistant Professor
LIET, Chikani, Alwar-Rajasthan

Abstract - A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without any fixed and preexisting infrastructure in which each node can act as a router. In MANET, both legitimate as well as malicious nodes are there. In this paper, the current security issues in MANET are investigated. Particularly, we have examined different routing attacks, such as blackhole, impersonation, wormhole etc. These attacks are the major problem in MANET because of different factor in MANET

1. INTRODUCTION

The ad hoc networks provide ubiquitous connectivity without the need of fixed infrastructure [1]. This makes them very suitable choice when the communication has to be provided temporarily such as in case of battle field, disaster hit area or to create a network between members of an interim group. Such a network is composed of mobile nodes which are powered by the battery. Therefore energy is a precious resource for all the nodes participating in the communication process and has to be used very carefully spent by every node who intends to stay alive in the network. The communication in the ad hoc network takes place using the concept of forwarding where a source node sends a packet to a far off destination node using intermediate relay nodes. This mechanism of transmission through relay node leads to the better connectivity and lower cost of power transmission than in case of direct transmission over large distance. Since the traffic in an ad hoc network is through the relay nodes hence it is desirable that every node participating in the network faithfully forwards the packets which it receives but is meant for some other node as destination. If such cooperation is received from every node in the network it would be an ideal situation. But like all other aspects of real life here also the conditions are not ideal and there exists non cooperative nodes in the network. These nodes may have two reasons for their non cooperation: malicious attitude or selfish attitude [2]. The malicious attitude of a node can be due to the opponent's intervention in the network where it intends to sabotage the network activity. The selfish attitude may be due to the various reasons where legitimate node in the network starts avoiding the forwarding activity due to its current low power status or it feels so over utilized in the forwarding activity and it fears that it will drain so much power that it will not have enough energy to send or receive its own packets in the future.

II. ATTACK CHARACTERISTICS

Dynamic topology, distributed operation, and resource constraints are some of the unique characteristics that exist in the ad hoc networks, which inevitably increase the vulnerability of such network. Many characteristics might be used to classify attacks in the ad hoc networks. Examples would include looking at the behavior of the attacks (passive vs. active), the source of the attacks (external vs. internal).

Passive vs. active attacks

Passive attacks are launched to steal valuable information in the targeted networks. Examples of passive attacks in ad hoc network are eavesdropping attacks and traffic analysis attacks. Detecting this kind of attack is difficult because neither the system resources nor the critical network functions are physically affected to prove the intrusions [3]. While passive attacks do not intend to disrupt the network operations, active attacks on the other hand actively alter the data with the intention to obstruct the operation of the targeted networks. Examples of active

attacks comprise actions such as message modifications, message replays, message fabrications and the denial of service attacks.

External vs. internal attacks

External attacks are attacks launched by adversaries who are not initially authorized to participate in the network operations. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually initiated by the external attackers.

More severe attacks in the ad hoc networks might come from the second source of attacks, which is the internal attack. Internal attacks are initiated by the authorized nodes in the networks, and might come from both compromised and misbehaving nodes.

Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the ad hoc networks. Security requirements such as authentication, confidentiality and integrity are severely vulnerable in the ad hoc networks with the compromised internal nodes because communication keys used by these nodes might be stolen and passed to the other colluding attackers. On the other hand, nodes will be classified as misbehaving if they are authorized to access the system resources, but fail to use these resources in a way they should be [4]. Internal nodes might misbehave to save their limited resources, such as the battery powers, the processing capabilities, and the communication bandwidth. Attacks that are caused by the misbehaving internal nodes are difficult to detect because to distinguish between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

III. SECURITY ATTACKS

Routing is one of the most vital mechanisms in the ad hoc networks. Improper and insecure routing mechanisms will not only degrade the performance of the ad hoc networks, but will also render such networks vulnerable to many security attacks. Most of the attacks is on the message, which is used to establish and maintain relationships between nodes in the networks. Attacks against the routing messages could be launched in many forms and may include all the characteristics described earlier. Information or messages could be deviated from the normal operation flow using modification, interception, interruption or fabrication attacks.

In a more severe case, attackers also might use any combination of these attacks to disrupt the normal information flow. As far as our concern, this study is the first to address security attacks against the ad hoc networks routing messages.

Modification

In a message modification attack, attacker makes some changes to the routing messages, and thus endangers the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the random relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks. Examples of attacks that can be classified under the message modification attacks are impersonation attacks and packet misrouting:

1) *Impersonation attacks: Impersonation* attacks are also called *spoofing* attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the intruder may even be able to reconfigure the network so that other attackers can (more) easily join or he could remove security measures to allow subsequent attempts of invasion. A compromised node may also have access to encryption keys and authentification information. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by modifying routing information [5].

2) *Packet misrouting attacks*: In a packet misrouting attack, malicious nodes reroute traffic from their original path to make them reach the wrong destinations . Attackers might misroute a packet to make it stay in the network longer than its lifetimes, thus render it to be dropped from the network. As a result, the source node needs to retransmit the lost packets and this will consume more bandwidth, as well as increasing the overhead in the networks.

Interception

Attackers might launch the interception attacks to get an unauthorized access to the routing messages that are not sent to them. These kinds of attack jeopardize the integrity of the packets because such packets might be modified before being forwarded to the next hop. Besides, the intercepted packets might also be analyzed before passed to the

destination thus violating the confidentiality. Examples of attacks that can be classified under the interception attacks are wormhole attacks and black hole attacks

1) *Wormhole attacks:* In the wormhole attacks, a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two colluding attackers are usually transmitted using wired connection to create the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operations.

2) *Black hole attacks*: In this attack, malicious nodes trick all their neighboring nodes to attract all the routing packets to them. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighboring nodes as having the most optimal route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its neighboring nodes.

Fabrication

Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause confusion in the network operations. They could launch the message fabrication attacks by injecting huge packets into the networks such as in the sleep deprivation attacks. However, message fabrication attacks are not only launch by the malicious nodes. Such attacks also might come from the internal misbehaving nodes such as in the route salvaging attacks.

1) *Sleep deprivation attacks*: This kind of attack is actually more specific to the mobile ad hoc networks. The aim is to drain off limited resources in the mobile ad hoc nodes (e.g. the battery powers), by constantly makes them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be launched by flooding the targeted node with unnecessary routing packets. For instance, attackers could flood any node in the networks by sending a huge number of route request (RREQ), route replies (RREP) or route error (RERR) packets to the targeted node. As a result, that particular node is unable to participate in the routing mechanisms and rendered unreachable by the other nodes in the networks.

2) *Route salvaging attacks*: Route salvaging attacks are launched by the greedy internal nodes in the networks. In a mobile ad hoc network, there is no guarantee that each transmitted packet will successfully reach the desired destination node . Packets might not reach the destination node because of the natural network failures or might be under attacks by the adversaries. Therefore, to salvage their packets from such failures, misbehaving internal nodes might duplicate and retransmit their packets although no sending error messages received. The effects of the route salvaging attacks might be more severe if there are many greedy nodes in the networks. Besides draining off more resources in intermediate and destination nodes, this attack might also cause the consumption of unnecessary bandwidth.

Interruption

Interruption attacks are launched to deny routing messages from reaching the destination nodes. Adversaries could do this by either attacking the routing messages or attacking the mobile nodes in the networks. Actually, most of the attacks launched in the modification, interception, and fabrication attacks are aimed to interrupt the normal operations of the ad hoc networks. For instance, adversaries aiming to interrupt the availability service in the networks might destroy all paths to a particular victim node by using the message modification attacks. In a message fabrication attack, adversaries could overload the networks by injecting huge unnecessary packets. Examples of attacks that could be classified under the interruption attacks category are packet dropping attacks, flooding attacks, and lack of cooperation attacks.

1) *Flooding attacks:* Adversaries also might interrupt the normal operations in the packet forwarding process by flooding the targeted destination nodes with huge unnecessary packets. Nodes under the flooding attacks are unable to receive or forward any packet thus all the packets directed to them will be discarded from network.

2) *Lack of cooperation attacks*: Lack of cooperation from the internal nodes to participate in the network operations can also be seen as an attempt to launch a refusal of service attack. In such attacks, internal nodes are discouraged to cooperate in the network operations that did not benefit them because participating in such operations will drain off their resources. Misbehaving internal nodes might use different strategies to save their limited resources. They might refuse to forward the other node's packets, not send back the route error report to the sender when failing to forward packets, or might turn off their devices when not sending any packet in the networks.

IV. CONCLUSION

In this paper, one can see that there are several attack characteristics that must be considered in designing any security measure for the ad hoc network. By investigating the characteristics and variations of the attacks, one can make a long list of attacks that could be launch against the ad hoc networks. However, since this study is focusing on the vulnerabilities of the ad hoc networks routing protocols, only some of the common attacks that could be launched against the ad hoc network routing protocols have been investigated. From the investigation, we identified that most of the common attacks against the ad hoc networks routing protocols are actually launched by exploiting the routing messages. From there, we further classify attacks against the routing protocols based upon the techniques that could be used by the attacker to exploit routing messages. In a future work, several security solutions that have been proposed to secure routing protocols will be investigated and classified based on this classification. The investigation will include various techniques that might be employed in protecting, detecting, and responding to the attacks against the routing message.

REFERENCES

[1] JosephMacker and Scott Corson. Mobile ad-hoc networks (MANET).http://www.ietf.org/proceedings/01dec/183.htm, December 2001.

[2] Shin Yokoyama, Yoshikazu Nakane Osamu Takahashi, Eiichi Miyamoto, "Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods", Proceedings of the 7th International Conference on Mobile Data Management (MDM'06)

[3] S. Bouam and J. B. Othman, “Data Security in Ad hoc Networks using MultiPath Routing,” in Proc. of the 14th IEEE PIMRC, pp. 1331-1335, Sept. 7-10, 2003.

[4] S. Ghazizadeh, O. Ilghami, E. Sirin, and F. Yaman, “Security Aware Adaptive Dynamic Source Routing Protocol,” In Proc. Of 27th Conference on Local Computer Networks, pp. 751-760, Nov. 6-8, 2002.

[5] Latha Tamilselvan, Dr. V. Sankaranarayanan **“**Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks” IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007.