RESEARCH REVIEW JOURNALS
Volume-03
Issue-12
December -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Survey of Security Issues in MANET

A.Priyadharshini

Assistant Professor, Dept of Information Science and Engineering, CMR Institute of Technology, Bangalore, Karnataka (India)

ARTICLE DETAILS

Article History
Published Online: 10 December 2018

Keywords
Routing attacks, Extended Dempster Shafer theory, OLSR

***Corresponding Author**
Email: priyadharshini.a[at]cmrit.ac.in

ABSTRACT

Mobile Ad hoc Networks are widely used in defense applications where traditional wireless network is difficult to implement as the network is formed by autonomous and decentralized wireless nodes. Privacy and Security in MANET are the most important disquiet for basic functionality of the network. Security is the major challenge in MANETs because of its characteristics like resource constraints, open medium, lack of fixed infrastructure, dynamism of topology and no clear security mechanism. As the topology is dynamic, routing process is very difficult. So MANET often suffers from routing attacks. In this paper, I provide a brief survey of attacks in MANET.

1. Introduction

In recent years the emergency of mobile devices and wireless have simulated research on self-organizing networks that do not require a centralized administration and predefined infrastructure. Ad hoc networks can be subdivided into two classes, one is static and another one is dynamic. The position of the nodes are fixed in static ad hoc networks and it can't be changed. But the position of the nodes can change frequently in Mobile Ad hoc networks.

MANET is a self-configuring infrastructure less network with mobile nodes connected without any physical link. Each node (device) in the MANET move independently in any direction and at any time any node can join or leave the network. All the nodes in the network act as both routers and end systems. Mobile Ad hoc Networks are utilized to structure wireless communication in locations without a predefined or centralized administration. Another distinctive characteristic of MANET is the dynamic nature of its network topology that is caused because of the unpredictable motion of the networking nodes. As each node acts as a router while transmitting data in MANET, the most common attack that affects MANET is routing attacks. So routing in MANET has become as a more challenging task.

There are many challenges in MANET. They are

i. Secrecy: The main objective of secrecy to protect information from unauthorized access.
ii. Authorization: Authorization is the process of specifying access privileges of a person. For eg. If a person is logged in into a system then specifying the person is having read rights or writes rights etc.
iii. Authentication: The major aim of authentication is to verify that the communicating entity is the one that claims to be.
iv. Non-repudiation: It protects the network or the system from denial by any one of the communicating entities.
v. Integrity Control: It provides the assurance that the data received are actually sent by the authorized person and are not modified while transmitting.
vi. Privacy: Keep systems from finding out about users.
vii. Confidentiality: It ensures that only the intended sender and receiver should be able to access the contents of a message.
viii. Access Control: The major principle of access control determines who should be able to access what.
ix. Availability: The main objective of availability is to ensure that the resources are always available to authenticated users.

2. Classification of attacks on MANET

Attack is an intelligent act that launch attempt to equivocate security services and infringe the security policy of a system. In general two types of attack are there, first type of attack is Passive attack: In passive attack the attacker tries to learn or read the message contents and won't try to alter them. Second type of attack is Active attack: In active attack the attacker tries to modify, insert, and delete the contents of the message. The attacks are further classified into insider attack and outsider attack. In insider attacker the attack initiated by an entity inside an organization and in outsider attack the attack is launched by a system outside an organization i.e by an unauthorized person. Among these attacks the attack that causes significant damage to MANET is routing attack.

A. Routing Attacks

The attacker node overflows the network with fake route creation packets to bogus (non existing) nodes or simply sends excessive route advertisements to the network. Routing in such a network is more challenging because of the dynamism of the network topology. So attacker can easily launch an attack.

Attacks during route discovery:

The attacks that target the route discovery phase such as routing table overflow, routing message flooding attacks, routing loop ,routing cache poisoning, etc.

Attacks during route maintenance:

In this type of attack the attacker target the route maintenance phase by broadcasts false control messages such as link-broken error messages which cause the solicitation of the costly route maintenance or repairing operation. Here the attackers send false route error messages to launch attacks.

Attacks during data forwarding phase:

In the data forwarding phase the attacker will launch attack while forwarding the data packets. The attackers do not forward data packets according to the routing table. Malicious nodes replay, flood data packets, simply drop data packets or modify data content.

Attacks on routing protocols:

In this type of attacks the attacker will target the routing protocols itself. For example in AODV (Ad hoc On-Demand Distance Vector) routing protocol the attacker will advertise a route with shortest path to the destination than the original shortest path. In DSR (Dynamic Source Routing) the attacker may modify RREQ(route request) or RREP(route reply) packets.

Wormhole Attack:

In this attack two attackers will cooperate and launch the attack. One attacker will record the routing traffic in one side of the network and tunnels it another point of the network and selectively inoculates tunnel traffic back into the network. This tunnel between two cooperating attackers is referred as a wormhole and this type of attack is called as wormhole attack.

Black hole Attack:

The attacker node injects false route replies to the route requests of the node it want to intercepts by pretending to have the feasible path to the destination claiming whose packets it wants to intercept. Now the attacker node can insert, alter or delete any data that have been routed through it.

Byzantine attack:

In this attack a compromised node or set of compromised nodes will be used to launch attacks such as forward packets through non-optimal paths selectively drop packets or routing loops

Node repudiation:

In this type of attack the communicating entities denies that they didn't send or receive a particular message.

Rushing attack:

If a fast transmission path occurs between two ends of a wormhole the tunneled packets can propagate faster than through a normal attacker fewer routes and it is known as rushing attack. Route discovery for the target node is initiated by the attacker node. If the neighbor of the target has received ROUTE REQUEST by the attacker first then a hop through the attacker will be included in the route that has been discovered.

Resource Consumption attack (Sleep Deprivation):

The attacker node forces the neighbor node by repeatedly requests for either existing or non-existing destinations and the resources are consumed more.

Location disclosure attack:

In this type of attack the attacker can able to find the location and structure of the network by using simple observing approaches.

Flooding attack(Routing table overflow):

The attacker node sends bogus route creation packets to non-existing nodes in order to flood the network or simply sends unnecessary route advertisements to the network and flood the network.

Impersonation attack:

The attacker node sends false routing information by masking as trusted node and this attack impersonation attack as the impersonates a legitimate node.

Node isolation attack:

The attacker will isolate a node by preventing the link information of that node and other nodes will not able to send data to the nodes that have been isolated.

Routing table poisoning attack:

In this type of attack the attacker injects RREQ packet with high sequence number which results in selection of non-optimal routes, creation of routing loops and even the whole network is partitioned.

Blackmail:

The perceived information about the malicious nodes will be maintained as blacklist by the other nodes. An attacker may fabricate the list and will ask other nodes in the network to add the node that contains will report other nodes in the network to add the node that contains the blacklist as attacker node.

Snare attack:

In this attack the node will be physically compromised by the attacker and the compromised node could be used to lure a Very Important Node (VIN).

The Invisible Node Attack:

In this attack the attacker will launch the attack without revealing its identity and the attacker node is called as Invisible Node.

What makes a Network vulnerable?

Anonymity:

An attacker can indirectly attack a system from thousands of miles away from the system, its administrators, or users. Thus the budding attacker is safe from an electronic shield.

Many points of attack-both targets and origins

A simple computing system is self-contained unit. Access controls in one system will ensure the confidentiality of data on that processor.

However, when a file is suited in a network the file need to pass through many hosts or routers to reach the user.

Sharing

As networks allows sharing of resources, more users have the potential to access networked systems than on single computers.

Complexity of System

Reliable security is a risk factor to achieve sometimes impossible especially in systems that are not specially designed for security.

Two or more possibly dissimilar operating systems will be combined by a network. Therefore, a network operating system is likely to more complex than an operating system for a single computing system.

Unknown perimeter

The uncertainty about the network boundary will also implied by a network's expandability.

A node can be part of two networks so information of one network can be traced by other network.

Unknown Path

There may be unknown paths between hosts.

Who attacks Networks?

Challenge

The persons who are skilled in writing or using programs have no dependency in the situation. Intellectual challenge is the most significant challenge for the attacker.

The attacker is fascinated to know whether he/she can defeat the network, and the response of trying a approach or technique.

Fame

For some attackers, the challenge of accomplishment is enough. But some attackers will except recognition for their activities.

That is, part of the contest is doing the deed; another part is taking credit for it.

The attackers use pseudonyms by retaining anonymity, but they achieve fame nevertheless. They may not be able to swank too openly, but they still likes to see their attack activities that is very interestingly discussed in social medias. Money and Espionage

Attackers can also be motivated by financial rewards too. As in other settings, attackers will be motivated by financial rewards too. Some attackers perform industrial espionage, seeking information on a company's long range plans products or clients.

Organized Crime

With potential revenue in the millions of dollars and attacks involving thousands of credit card numbers and other pieces of identity, existing organized crime units are sure to take notice.

Ideology

Hactivism

Hactivism involves disturbing the normal operations of the network by normal hacking techniques. This won't cause any serious damage.

Cyberterrorism

Cybeterrorism is more dangerous than hactivism, this may cause more deviating damage such as loss of life or heavy economic damage by politically motivated hacking operations. Reconnaissance

Attackers do not eventually sit down at a terminal when they want and then launch an attack. An intelligent attacker will plan and investigates before launching the attack.

Port Scan

It involves in designing a program that is used to gather information about a particular network, and gives reports and ports respond to messages and vulnerabilities seem to be present which of several known.

Pinging

The fastest way to determine if a host is alive is to ping it. The ping command used for this purpose, sends out an ICMP(Internet Control Message Protocol) echo request, causing the target to respond with an ICMP replay packet.

Countermeasure

i) Configure the firewall to drop incoming ICMP echo requests and outgoing ICMP echo replies.
ii) Prevent TCP ping scans.
iii) Configure the firewall to drop packets designated for closed ports.
iv) Configure the firewall to not trust source port values.

3. Conclusion

A variety of intrusions in MANET has been surveyed in this paper. And possible countermeasures for every attack has been proposed. A common approach to overcome all this attacks is to hybrid cryptographic techniques. Instead of detecting the attack after its arrival preventing the attack will be more effective. So an Intrusion Prevention and Detection System(IDPS) will be more effective intrusion handling tool for the MANET.

References

1. P. Cheng, P. Rohatgi, C. Karger, G. Wagner, and A. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc.28th IEEE Symp.Security and Privacy, 2007.
2. T. Clausen and P. Jacquet "Optimized Link State Routing Protocol (OLSR)," RFC 3626,IETF Network Group,October 2003.

3. P.Jacquet, A. Laouiti,P. Minet and L. Viennot “Performance of multipoint relaying in ad hoc mobile routing protocols,” Networking 2002. Pise (Italy) 2002.
4. Y. Zhang and W. Lee,“Intrusion detection in wireless ad-hoc networks,” in Proceedings of Mobicom 2000,pp.275-283,Aug 2000.
5. H. Deng, W. Li, and D.P. Agrawal, “Routing security in ad hoc Networks,” IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
6. C. Tseng, T. Song, P. Balaaubramanyam, C.Ko, and K. Levitt, “A Specification-Based Intrusion Detection Model for OLSR,” Proc. Ninth Int’l Symp. Recent Advances in Intrusion Detection (RAID ’06), pp.249-271,2006.
7. G. Shafer, A Mathematical Theory of Evidence, Princeton Univ., 1976.
8. Y. Sun, W. Yu, Z. Han, and K. Liu, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks,” IEEE selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.
9. L. Sun, R. Srivastava, and T. Mock, “An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions,” J. Management Information Systems, vol. 22, no. 4, pp. 109-142, 2006.
10. C. Mu, X. Li, H. Huang, and S. Tian, “Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory,” Proc. 13th European Symp. Research in Computer Security (ESORICS ’08),pp. 35-48, 2008.
11. K. Sentz and S. Ferson, “Combination of Evidence in Dempster-Shafer Theory,” technical report, Sandia Nat’l Laboratories, 2002, L. Zadeh,“Review of a Mathematical Theory of Evidence,” AIMagazine, vol. 5, no. 3, p. 81, 1984.
12. M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, “Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks,” IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719, May 2010.
13. S. Wang, C. Tseng, K. Levitt, and M. Bishop, “Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks,” Proc. 10th Int’l Symp.Recent Advances in Intrusion Detection (RAID ’07), pp. 127-145, 2007.
14. C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On-Demand Distance Vector Routing,” Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.
15. H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, “Sensor Fusion Using Dempster-Shafer Theory,” Proc.IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.

