ISSN:0975-9646

MANET: Security and Challenges

Tripathi Lalit Kumar
CSE.,
United institute of technology Naini Allahabad, India

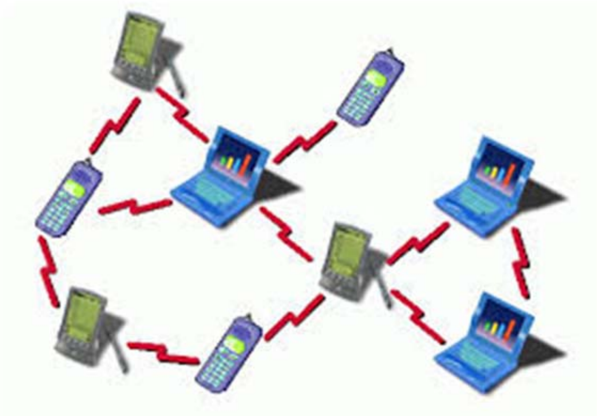
Dr. Kanojia Sindhuben
Asst. Prof. (CSE)
United institute of technology Naini Allahabad

Abstract-**Mobile ad hoc network is a collection of mobile nodes with no pre-determined network infrastructure. Security is an important aspect in wireless ad-hoc network. The nodes possess an exclusive characteristics and it leads to significant challenges to security. A d hoc network is dynamic and these networks become vulnerable to many number of attacks. We discussed in detail about security attacks, parameters and challenges.**

INTRODUCTION:

MANET is dynamically establishing mobile nodes networks with no fixed infrastructure. Each mobile node is equipped with wireless transmitter and a receiver with a suitable antenna. Nodes in mobile ad hoc networks move freely in the network and they can organize themselves in a random way. The important sector of ad-hoc network is routing protocols because network topologies keep on changing due to the movement of the nodes. All the network related activities like discovering of topology and delivery of packets is performed by the nodes itself. The nodes communicate over wireless links; they have to compete with the effects of radio communication, such as noise and interference. In Manet the links typically have less bandwidth than a wired network. Each node in a wireless ad hoc network functions as a host as well as a router. The control of the network is distributed among all the nodes of the network.

The aim of this paper is to provide a brief introduction of Manet security threats and analysis of its security challenges. Since each packet forwarded from one node to another node in the networks so each node must have trust to each participating nodes in the traffic of communications. If threats act on routing protocols one is form nodes that are not part of the network and other from inner that are part of the network due decentralized network it faced lots of challenges.



Basic Diagram of Mobile ad hoc network

BASIC CHARACTERISTICS OF AD HOC NETWORKS

1) No fixed infrastructure: An ad-hoc network is a collection of nodes that do not depends on fixed infrastructure for connectivity of the nodes. Hence these types of networks are flexible and effortlessly reconfigurable.
2) Limited resources: These networks have limited resources for their computational actions. Resources like battery power, bandwidth, computation power, memory etc have to be used wisely and efficiently for the endurance and proper operation of the network.
3) Dynamic Topology: In ad hoc networks Nodes are free to move arbitrarily, wireless devices like Laptops, PDAs, smart-phones etc. due to frequent change in their location results the dynamic topology of it.
4) Autonomous Networks: it is also known as stand-alone self-organized network Due to their decentralized nature these networks have lesser complexities of infrastructure setup, enabling devices to create and join network wherever, anytime, for any kind application. A node in the ad hoc networks can communicate with all other nodes that are in its transmission range. Nodes in the network are self-sufficient for the purposes like routing packets and assuring security of the network and so on.

IMPORTANT PARAMETERS IN MANET SECURITY

Since MANET’s have special characteristics, there are some important metrics in MANET security that are important in all security approaches; we call them “Security Parameters”. Being unaware of these parameters may cause a security approach useless in MANET. Each security approach must be aware of security parameters All mechanisms proposed for security aspects, must be aware of these parameters and don not disregard them; otherwise they may be useless in MANET. Security parameters in MANET are as follows:

Network Overhead: This parameter refers to number of control packets generated by security approaches. Due to shared wireless media, additional control packets may easily lead to congestion or collision in MANET. Packet lost is one the results of congestion and collision. Therefore, high packet overhead increases packet lost and the number of retransmitted packets. This will easily wastes nodes energy and networks resources.

Processing Time: Each security approach needs time to detect misbehaviors and eliminate malicious nodes. Due to MANET’s dynamic topology it is strongly possible that routes between two different nodes break because of random mobility of the nodes. Therefore, security approaches must have low processing time in order to enhance MANET flexibility.

Energy Consumption: In MANET nodes have limited energy supply so optimizing energy consumption is extremely challengeable issue in MANET. High energy consumption reduces lifetime of the nodes as well as network.

All security protocol must be aware of these important parameters. In some situations a trade-off between these parameters is provided in order to perform a satisfaction level in all of them. Security protocols that pay no attention to these parameters are not efficient as they misuse network resources.

SECURITY SERVICES

The aim of a security service is to secure network before any kind of attack that encountered in the network and made it harder for a malicious node to breaks the security of the network. MANET providing these services faced lots of challenges. For securing MANET a trade-off between these services must be provided it means if any one service guarantees without taking account of other services that security system will fail. The problem is to provide services one by one in MANET and presenting a way to guarantee each service. We discuss about five important security services and their challenges as follows:

Availability: In this service, each authorized node must have access to all data and services in the network. Availability challenge arises due to MANET's dynamic topology and its open boundary. Accessing time, which is the time needed for a node to access the network services or data is important, because time is one of the security parameters. By using lots of security and authentication levels, this service is disregarded as passing security levels needs time.

Authentication: The goal of this service is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be in no doubt about identity of the source node. To provide this service it is using certifications; key distribution and key management are challengeable

Data confidentially: According to this service, each node must have access to specific services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods but in MANET there is no central management, key distribution faced lots of challenges and in some cases impractical

Integrity: According to integrity security service, only authorized nodes can create, edit or delete packets. As an example, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them.

Non-Repudiation: By using this service, neither source nor destination can repudiate their actions or data. It means if a node 1 receives a packet from node 2, and sends a reply to node 2 cannot repudiate the packet that it has been sent.

REASONS OF MANET BEING UNSAFE

i. **No central management** – Every node in MANET is self-configured and self-administered. Therefore it is difficult check or control the transfer of data.
ii. **Freedom for a** node – Any node in network is free to enter or leave the network so any malicious activity by a node cannot be tracked completely.
iii. **Low Power** – In a MANET every node is light weighted so with small battery backup and small memory size.
iv. **Data loss during transmission** – as both sender and receiver node are mobile there are frequent path breaks in MANET so possibility of data loss during transmission is high.
v. **Limited bandwidth** – Wireless network has much less capacity as that of wired network.
vi. **Trust issues with routing protocols** – As every node in MANET is independent, routing protocols assumes that all nodes present in network are non-malicious and cooperative.

TYPES OF NETWORK ATTACKS

Attacks on the ad hoc networks can be broadly categorized as Passive Attacks and Active Attacks.

i. Passive Attacks - The main aim of passive attackers is to steal the valuable information from the targeted networks. Attackers do not scare the normal network functioning like inducing false packets or dropping packets. They basically become a part of the network. They do not initiate any malicious activity to disturb the normal functioning of the network. It becomes very difficult to identify such kind of attacks. Examples of such types of attacks are traffic analysis, traffic monitoring and eavesdropping.

ii. Active Attacks - Active attackers tamper the network traffic like cause congestion, propagation of false routing information etc. Due to active participation of attackers, their detection and prevention can be done using appropriate prevention algorithms. Examples of passive attacks include modification attack, impersonation, fabrication and message replay.

Attacks can also be classified depending upon the position of the attacker in the network.

i) External attacks

External Attacks are the attacks made by the unauthorized nodes which are not a part of the network. External attackers can flood false packets in the network, impersonation etc. Their aim of such attackers is to cause congestion or to disturb expected network functioning.

ii) Internal attacks

Internal attacks are caused by the internal nodes in the network. The reason for their malicious behavior may be the following:

a) Hijacking those (authorized) nodes by some external attacker and then using them for Launching internal attacks in the network.

b) Selfishness to save their limited resources like battery power, processing capabilities, and the Communication bandwidth and exploiting other nodes for their benefit.

ATTACKS IN MANET

Due to special features like hop- to-hop communications, wireless medium, and easy to setup, MANET became popular for malicious nodes. Some of the most important attacks in MANET are as follows:

Black Hole Attack: In this attack, malicious node injects fault routing information to the network and forward packets toward it and then discards all of them. In black hole attack the attacker node advertises itself to other node that it has shortest route to reach towards destination. If this reply reaches before the actual reply an artificial route will be established that also includes the malicious node of the network. Now this malicious node can drop packets. The Throughput and the packet to delivery ratio of the AODV protocol using black hole attack can be analyzed by introducing an attacker on a particular node. Whenever an attacker claims for a specific node, there is a possibility that several parameters like throughput, packet to delivery ratio etc can vary accordingly [15].

Worm Hole Attack: In worm Hole attack, malicious node records packets at one location of the network and tunnels them to another location. Fault routing information could disrupt routes in network. Authors in presented a way to secure MANET in opposition to this attack by using encryption and location information of the node. But as mentioned before, key distribution is a challenge in MANET. Packet leash [5] is a technique for detecting and defending against wormhole attacks. A leash is any information on that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Till now various techniques have been proposed for prevention and detection of wormhole attack. In [12], in this paper the impact of wormhole attack is decrypted and concise detail of wormhole attack and its types are explained. Also present various detection and prevention techniques are discussed.

Byzantine attack: In this attack, malicious node injects fault routing information to the network, in order to locate packets into a loop. One way to protect network against this attack is using authentication. Authors in presented a mechanism to defeat against this attack using RSA authentication. In [17] once t active set of insider nodes in the network are turned to be malicious by threats then the whole network will be under the control of adversaries and further secured data transmission is not possible. This is very critical in mobile devices used in military fields and medicinal fields to transferring patient reports and medical advises. A byzantine adversary can prevent the route establishment by dropping the route call or response packets and modify the route selection metrics such as packet ids, hop counts, drops packets selectively.

Denial of service: In this attack, malicious node prevents other authorized nodes to access network data or services. Using this attack, a specific node or service will be inaccessible and network resources like bandwidth will be wasted. [3] Although many efforts (including above) have been done on the impact of Denial of Service attacks in MANETs, few of them analyzed the impact on the connectivity, which is an essential requirement for any networks, especially military networks

Jamming attack: Jamming attack is a kind of DOS attack. The aim of a jammer is to interfere with legal wireless communications. It can achieve this goal by preventing a real traffic source from sending out a packet and by preventing the reception of legitimate packets.

Modification Attack: In this attack, malicious nodes sniff the network for a period of time. Then, explore wireless frequency and use it to modify packets. Man-in-the-middle is a kind of Modification attack.

Man-in-the-middle attack: In this attack, malicious node puts itself between source and destination. Then, captures all packets and drops or modifies them. Hop by hop communications are made MANET vulnerable against this attack. Authentication and cryptography are the most effective ways to defeat this attack.

CONCLUSION

In this paper we discussed various Security Aspects of MANETs .we done literature survey for detecting the malicious nodes misbehaviors in mobile ad hoc network. Ad-hoc networks are proven to various kinds of vulnerable attacks since they are dynamic, wireless and infrastructure network. We have found that necessity of secure routing protocol is still a very strong question. There is no universal algorithm available that suits well against the most generally known attacks. However, in short, we can say that the complete security solution requires the prevention, detection in MANET.

REFERENCE

[1] Debarati Roy Choudhurya Dr.Leena Ragha Prof. Nilesh Marathe "Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack" International Conference on Advanced Computing Technologies and Applications (ICACTA-2015)

[2] Shikha Jain "SECURITY THREATS IN MANETS A REVIEW "International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014

[3] "Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks ".Fei Xing Wenye Wang Department of Electrical and Computer Engineering North Carolina State University , Raleigh, NC 27695, USA

[4] K.U. R. Khan, R. U. Zaman, and A. V. G. Reddy, "Integrating Mobile Ad Hoc Networks and the Internet challenges and a review of strategies," presented at the 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE, 2008.

[5] Akansha Shrivastava and Rajni Dubey “Wormhole Attack in Mobile Ad-hoc Network” International Journal of Security and Its Applications Vol.9, No.7 (2015), pp.293-298

[6] H.Nishiyama, T. Ngo, N. Ansari, and N. Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks," Wireless Communications, IEEE Transactions, 2012.

[7] Nishu Garg R.P.Mahapatra “MANET Security Issues” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009

[8] Adamson, B., "Tactical Radio Frequency Communication Requirements for IPng", RFC 1677, August 1994.

[9] Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, “A secure routing protocol for Ad-hoc networks,” Proc. Of IEEE ICNP, 2002

[10] Zhou L. and Haas Z.J, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no. 6, 1999

[11] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks”, IEEE Networks, Volume 13, Issue 6 1999

[12] Ajay prakash ,vineet etc “wormhole attack Detection in mobile ad hoc network” JIEIT vol. 2,issue 2 aug 2012

[13] J. Godwin Ponsam ,Dr. R.Srinivasan “A Survey on MANET Security Challenges, Attacks and its Countermeasures” International Journal of Emerging Trends & Technology in Computer Scien ce (IJETTCS)

[14] Praveen Joshi “Security issues in routing protocols in MANETs at network layer” Procedia Computer Science 3 (2011) 954–960

[15] Praveen KS Gururaj &Ramesh”comperative analysis of black hole attacks in ad hoc network in AODV &OSLR protocol” International Conference on Computational Modeling and Security (CMS 2016)

[16] Rashmi Mahajan , Prof. S. M. Patil“ A Review of ‘MANET’s Security Aspect and Challenges with Comprehensive Study of SIDS for Discovering Malicious Nodes” IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.

[17] Geetha.A, and Sreenath.N “Byzantine Attacks and its Security Measures in Mobile Adhoc Networks” Int'l Journal of Computing, Communications & Instrumentation Engg. (IJCCIE) Vol. 3, Issue 1 (2016) ISSN 2349-1469 EISSN 2349-1477