Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.365 – 370

REVIEW ARTICLE

A Review: Security Issues in Mobile Ad Hoc Network

Priti[1*], Dr. Priti Sharma[2]

[1]M.Tech Student, Department of Computer Science and Applications, M. D. University, Rohtak-124001, Haryana, India

[2]Lect. Department of Computer Science and Applications, M. D. University, Rohtak-124001, Haryana, India

[1] priti.dhandhi@gmail.com*, [2] pritish80@yahoo.co.in

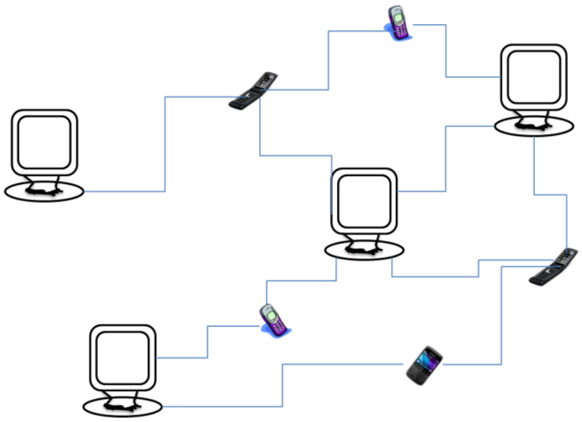
Abstract: ***Mobile Ad-hoc network is infrastructure less, spontaneous and multi-hop network, which consist of decentralized wireless mobile nodes. MANET uses temporary ad-hoc network topologies, that allowing people and devices to seamlessly connect to network in areas with no pre-existing communication infrastructure e.g. disaster recovery environments. And mobile ad-hoc network is a collection of nodes that are connected through each other with a wireless medium forming rapidly changing topologies. Routing in mobile ad-hoc network is a challenging term due to its dynamic changes in topologies. There are lots of trust models and routing protocol which are used in MANETs to get a security. Various trust schemes are used to provide integrity, confidentiality and availability in mobile ad-hoc network to gain the secure environment. In this paper, we will discuss characteristics, attacks and security in mobile ad-hoc network.***

Keywords – Mobile ad-hoc networks, applications, attacks, security

Introduction

A Mobile ad-hoc network (MANET) is wireless systems which consist of mobile nodes that are dynamically communicate to each other over a wireless channel. Mobile ad-hoc networks are collection of various wireless networks like sensor network, cellular network, which consist of large number of mobile nodes. Nodes in MANETs can join and leave the network according to their requirements. In this network, there is no fixed set of infrastructure and centralized administration. The changeable nature of this type of networks makes it highly susceptible to various link attacks. The basic requirement for a secured networking is powerful and secure routing protocol which insures the integrity of network, availability authenticity and confidentiality. Many previous security solutions for the wired networks are ineffective and inefficient for MANET environment.

As the transmission take place in open medium network then it makes the Mobile ad-hoc network is more vulnerable to security attacks. Various attacks can be reduced due to the presence of security protocols. In MANET speed varies according to the applications, for example, in military application speed is low (long range network) but in commercial application speed is high (short range network) i.e. speed is inversely prepositional to the network range. Over the wireless network, it consist two variations of network infrastructure and infrastructure less. The infrastructure networks, in which mobile nodes connect with an access point like base stations that are connected to fixed network infrastructure. The infrastructure less networks is other type of wireless networks, is knows as MANET. MANET has no fixed access points while every node could be router or host. MANETs lack prior organization and central administration, so security issues are different and thus require different security mechanisms. Wireless links in MANETs make it more prone to the attacks for attackers. Attackers can directly attack the internet to delete messages, add malicious messages. In this paper, we will discuss different attacks and security issues of MANETs.



Mobile Adhoc Networks

Characteristics and Applications

MANET has various characteristics-

1. Absence of infrastructure- Mobile ad-hoc networks are supposed to operate independently of any fixed infrastructure.
2. Inferior link capacity- The scalability, reliability, efficiency and capacity of wireless links are often inferior when compared with wired links. Source to destination path can be shared by several sessions.
3. Multi-hop transmission-when a sender node and receiver node for a message is out of the transmission range, then the MANETs are capable of multi-hop transmission. When delivering

the messages from source to its destination out of the transmission range, the messages have to be forward through more intermediate nodes.

4. Dynamically changing topologies- In MANET, the change in topologies is frequent and dynamic in nature. The connectivity between nodes may vary with time and dynamically establish routing between them.
5. Light weight features- MANET nodes are mobile devices with small memory size, less CPU processing capability and low power storage.
6. Autonomous behavior- Into the MANETs, every node behaves as a router or as a host. It means that a node has ability of host and can also perform switching functions as router so endpoints and switches are indistinguishable.
7. Symmetric environment- All nodes have various features with similar capabilities and responsibilities. And all nodes perform same functions over the network.

MANET include in various applications-

1. Commercial sector- MANET can be used in emergency operations for natural hard problems relief effort, e.g. in earthquake and flood etc. Rescue operation must take place when non pre-fixed or damaged communication infrastructure is needed.
2. Personal area network- wired cables are replaced by wireless connections. Short-range MANET can simplify the communication among many mobile devices for examples laptop, mobile phones and wearable computers. And MANETs can extend to access the internet easily by various mechanisms.
3. Military battlefield- military equipment contains some sort of computer equipments. Through MANET networking; the military could take the advantage of common place network technology and maintain information between headquarters, vehicles and soldiers.

Attacks on MANET

In MANET, there are different kinds of attacks which are done by the attackers which are always tries to reduce the performance of network. The Mobile Ad-hoc network is more vulnerable to various attacks not from outside but also from within the network itself.

There are two types of major attacks in MANET which are following as below.

(1) Internal attacks
(2) External attacks

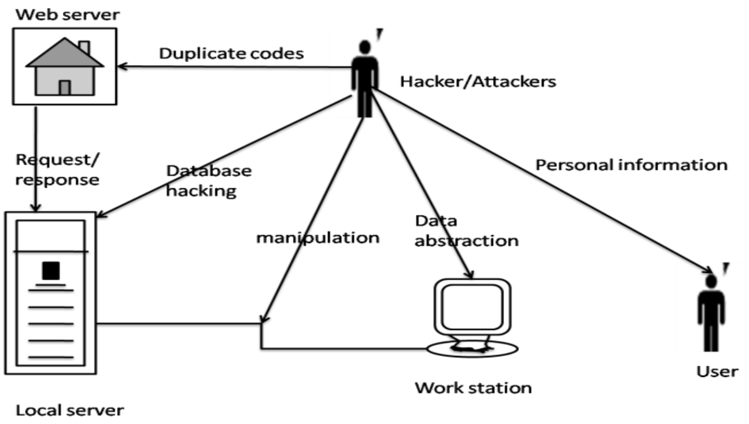
Internal attacks- These attacks are directly attack on that nodes which are worked in network already and also attacks on links interface between them. These internal attacks sometimes may broadcast wrong type of routing information to other nodes. And these types of attacks are more difficult to handle as compare to other attacks. The malicious nodes generate the wrong routing information so these nodes are more difficult to detect.

External attacks-External attacks are always tries create congestion in the network, advertising wrong routing information and denial of services etc. External attacks have two types**:**

1- Active Attacks

2- Passive Attacks

Active Attacks- active attacks are more dangerous on the network that prevents flow of messages between the nodes. And active attacks can be external or internal these attacks can be carried out by outside, which are belong to network. Internal attacks are malicious nodes that are part of the network, internal attacks are more difficult to detect than the external attacks. The active attacks are launched by malicious nodes. Generally malicious nodes change the routing information by advertising itself as having a short path to the receiver.



How hackers/Attackers effect our works

Passive attacks- MANETs are more susceptible to passive attacks. Passive attack does not alter the data transmitted within the network because it includes unauthorized “listening” to the network traffic. Passive attacker does not destroy or change the operation of a routing protocol, but attempts to find the information from routed traffic. An encryption algorithm is used to encrypt the data being transmitted to overcome these types of attacks.

Security

There are several security criteria to secure the important information. These are as follows-

1. Confidentiality
2. Availability
3. Integrity
   a. Malicious altering
   b. Accidental altering
4. Authentication
5. Authorization
6. Non-repudiation
7. Attacks using fabrication

1. Confidentiality: - confidentiality is a term which is generally used to provide information only for those who have been authorized to access that accessible information. In some times we need to keep the information secret from all of the unauthorized node or because of this may be malicious nodes and can interrupt or destroy the information. So we have to maintain the confidential information from the unauthorized entity.

2. Availability: - availability is that security criteria in which an entity should maintain its ability into its security criteria for provide the all of the designed services. And into this term some malicious entities or nodes can make the service unavailable.

3. Integrity:-Integrity is a term in which information that will be transmitted, is never interrupt or destroy. It can be done in two ways.

(i) When the information is destroyed & replicated by an attacker with some malicious term, is called the malicious altering.

(ii) When the information is lost or its some elements are changed due to some kind failure, which may be transmission faults in authorization or hardware fault, then it called the accidental altering.

4. Authentication:- Into the authentication security criteria firstly insure that a node into the communication are not an unauthorized node or not impersonator. Sometimes into act the authentication term, the malicious node act as helpful node and thus tries to access the confidential information or can insert the faulty messages to interrupt the network process.

5. Authorization:- Any unauthorized person cannot behave like as the authorized person to access any confidential information. This is used to provide various different access rights to various types of users.

6. Non-repudiation:- Non-repudiation is a term that source and destination of an information cannot disavow that they have sent or received an information. This is useful at that time when we try to search about the malicious nodes which are always tries to interrupt the network operations between various authorized nodes.

7. Attacks using fabrication:- fabrication is a process in which false routing messages are generated . And there is very difficult to detect such types of messages.

Conclusion

MANET infrastructure is dynamic in nature and having no centralized administration that make this network is more vulnerable to many attacks. In this paper we have discussed various type of attacks and these are classified as active and passive attacks. In future, we will try to implement security algorithm along with routing protocols which help to reduce the effect of different attacks.

REFERENCES

[1] Robinpreet Kaur & Mritunjay Kumar Rai, Department of Electronics and Engineering, Lovely Professional University, Phagwara, Punjab, India "A Novel Review on Routing Protocols in MANETs" under Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012

[2] Lu Han, October 8, 2004 "Wireless Ad-hoc Networks"

[3] M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network," Ericsson Review, No.4, 2000, pp. 248-263.
[4] "THE HANDBOOK OF AD HOC WIRELESS NETWORKS" Edited by Mohammad Ilyas Florida Atlantic University Boca Raton, Florida
[5] Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County "Security Issues in Mobile Ad Hoc Networks- A Survey"
[6] 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
[7] Kisung Kim and Sehun Kim, "A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks".
[8] Ad hoc network specific attacks held by Adam Burg.
[9] Akanksha Saini, Harish Kumar, "Effect of Black Hole Attack on AODV Routing Protocol in MANET".
[10] Sevil ¸ Sen, John A. Clark, and Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks".