ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 4, Issue 3, pp: (245-250), Month: July - September 2016, Available at: www.researchpublish.com

An Overview of Mobile Ad Hoc Networks

[1]Saranya. A, [2]K. Rajasekaran, [3]Selin Chandra C S

[1,3]Research Scholar, Dept. of CS, D.B Jain College [Autonomous], Chennai, India
[2]Associate Professor, Dept. of CS, D.B Jain College [Autonomous], Chennai, India

Abstract: **MANET is a rapidly emerging mobile communication technology which offers fruitful services in various fields like military battle field, emergency services, entertainment, sensor networks, home and internetworking etc., Due to dynamic topology, open environment, infrastructure less network and lack of centralized administration MANETs are susceptible to various attacks. This paper describes the various types and tools of MANET and it presents an overview of MANET applications, technological challenges and different security attacks.**

Keywords: **Applications, Attacks, Challenges, MANET, Tools.**

I. INTRODUCTION

An ad-hoc network is a network that built spontaneously as devices connect. Instead of depending on a base station to control the flow of packets to each node in the network, the packets are sent to and from each other by the individual network nodes in ad-hoc. It does not require any access point. In Latin, ad-hoc literally means "for this", meaning "for this special purpose". For example, if Bob needs to transfer a file to Sally, Bob has to create an ad-hoc network with Sally's computer. This may do by using wired or wireless connection. If Bob needs to transfer files with more than one computer, he could set up a multi-hop ad-hoc network. Basically, ad-hoc network is a temporary connection created for a particular purpose. If the network is set up for a longer duration, then it is just a plain local area network. MANET is a type of ad-hoc network. Mobile ad-hoc network is a collection of mobile devices like smart phones, PDA, laptop etc., within a range, these kinds of mobile devices communicate with each other in a peer-to-peer manner using radio frequency. Since MANETs are self-configuring, self-healing, infrastructure less network they does not depend on any base station to co-ordinate their messages. In MANET the nodes in the network acts as a router to forward packets. MANET has various types which work for various purposes. Performance of MANET can be tested using various simulation tools. Mobile ad-hoc networks are applied in constantly changing locations where the wired connection is not possible. Example: Military battlefield. Since mobile ad-hoc network works in an open environment it is vulnerable to many active and passive attacks.

II. RELATED WORK

A MANET is a highly capable, rapidly growing and fast deployable wireless network topology. Limitations of infrastructure, self-creation, self-organization and self-administration are the characteristics of MANET. Researchers [2], [4] focused mainly on the challenges and applications of MANET. But, in this paper we have also discussed about the types of MANET and its simulation tools. In the end, we have described the major security attacks of mobile ad-hoc network.

III. TYPES OF MANET

A. VANETs:

Vehicular Ad-hoc Networks are used to make communication among vehicles and road side equipment by using the principle of mobile ad-hoc network, i.e. data exchange is done through wireless network.

B. InVANETs:

Intelligent Vehicular Ad-hoc Networks are applied in the field of road transport because it manages road traffic and mobility of vehicles by using artificial intelligence which helps the vehicles to move in intelligent manner during accidents, drunken driving etc.

C . SPANs:

Without depending on cellular carrier network, wireless access points or traditional network infrastructure, Smart Phone Ad-hoc Networks uses smart phones to create peer-to-peer network. It connects android phones through mesh network using Wi-Fi, which helps during emergency situations.

D. iMANETs:

Internet based Mobile Ad-hoc Networks connect mobile nodes and fixed Internet- gateway nodes i.e. multiple sub-MANETs are connected through a Hub- Spoke to create a widely distributed MANET. In such situation normal ad-hoc routing algorithm does not apply directly rather than we need to deploy Cloud Relay.

E. Tactical MANETs:

This type of ad-hoc network is used in military battle field, disaster and critical areas because of its flexibility, availability and survivability. It is used for remote navigation and control. Tactical MANETs require limited knowledge for deployment.

IV. APPLICATIONS

A. Military Battlefield:

Mobile ad-hoc networks are self-organizing, self-forming and self-healing network which requires no central administration. It enable the war fighter to focus on the mission rather than managing the network [3],[7].

B. Vehicular Service:

Vehicular Ad-hoc Network helps to connect and communicate vehicles and road side equipment. iVANET uses artificial intelligence to avoid vehicle –to-vehicle collision.

C. Coverage Extension:

Mobile ad-hoc network is used to extend the cellular network access and linking up with Internet and intranets.

D. Sensor Network:

MANET can be used to data track the environmental conditions, animal movements, chemical/ biological detection [2].

E. Emergency Services:

MANET creates a rapid communication network during emergency or rescue operation- disaster relief efforts like fire, flood or earthquake.

F. Personal Area Network (PAN):

Short range of mobile ad-hoc network forms PAN, which is a promising application field of MANET in the future computing world. [4]

G. Entertainment:

MANET is also applied in the field of entertainment by supporting multi-user games, outdoor internet access etc. It is used in audio video streaming which is helpful for live conferencing.

V. CHALLENGES

A. Dynamic topology:

The nodes in the MANET are free to move arbitrarily, thus the network topology may change randomly and rapidly at unpredictable times [7]. In MANET, nodes with poor security may misbehave and it reduces the network performance. Ex: war field.

B. Routing:

The issue of routing packets between any pair of nodes becomes a challenging task since the topology of the network is constantly changing. MANETs are typically multi hop, which is more than single hop communication [4].

C. Bandwidth Constraint:

When comparing to hardwired counterparts wireless links will continue to have significantly lower capacity which is more susceptible to external noise, interference and signal attenuation effects [10].

D. Quality of Service (QoS):

In a constantly changing environment, it is a challenge to provide different quality of service levels and it is difficult to offer fixed guarantees on the services offered to a device.

E. Security:

MANETs has no centralized administration and it works on an open environment. Providing security for such network is a difficult task.

F. Internetworking:

Internetworking between MANET and IP based fixed networks are often expected. It's a challenge to provide harmonious mobility management in the coexistence of routing protocols in such a mobile device.

G. Limited Resources:

Mobile communication devices like laptops, computers, smart phones are connected together to form mobile ad-hoc network. All these devices have different storage capacity, computational power and processing speed. This might attract the attackers to perform new attacks [9].

H. Channel Vulnerability:

Mobile ad-hoc network is vulnerable to eavesdropping, spoofing and denial of service attacks because mobile wireless networks are generally more prone to physical security threats than are fixed cable networks.

I. Power Supply:

Mobile nodes rely on batteries or other exhaustible means for their energy. Conservation of power is a difficult while forming MANET.

VI. SECURITY ATTACKS

MANETs attack can be classified into two categories: active attack and passive attack.

A. Active Attack:

This type of attack attempts to destroy the data being exchanged in the network by modifying the data stream or involved in the creation of false stream.

Active attack is further divided into two categories: internal and external.

- Internal attacks are from the compromised nodes that are presented in the network.
- External attacks are from the node that does not belong to the network.

Some of the active attacks are described below,

a) Black hole attack:

In this attack, a node advertises zero metric to all destinations making all nodes around it to route packets towards it. This malicious node, instead of forwarding the packets, it drops the entire packet that it receives. As a result, the amount of retransmission needed increases leading to congestion.

b) Wormhole attack:

In this type of attack, two malicious nodes joined together by forming a tunnel, this link is known as wormhole. This is unsafe and the wormhole detection is unsafe [8][11].

c) Rushing attack:

Each node before transmitting the data, establish a valid route to destination. RREQ (route request) message is broadcasted by the sender node and the valid route replies with RREP (route reply). Rushing attack exploits this mechanism and the attacker quickly forward with a malicious RREQ on behalf of original node. Due to the duplicate reply, the actual valid message will be discarded and consequently the malicious node becomes the part of the route. So this attacker node sends packets to proper node. This might actually increase the delay in packet delivery to the destination node.

d) Flooding attack:

Flooding attack floods the network with fake RREQ to block the network and to reduce the transmission of the real node.

e) Byzantine attack:

Set of intermediate nodes or intermediate nodes work together to carry out attacks such attacks such as creating routing loops, forwarding packets on non-optimal path results in disruption of routing services within the network.

f) Sinkhole:

In this the node eaves drops all the data that is being communicated between its neighboring nodes. This attack can be implemented on ad-hoc network such as AODV protocol using computation for reducing hop count and maximizing the sequence network, this malicious node appear to be the best available route for the nodes to communicate.

g) Sybil attack:

This attack disturbs the communication among the node of the network by using several identities at a time and increases lot of misjudgment among the nodes in the network. It may use identity of other nodes present in the network and create false impression of that node in the network [11].

h) Jamming:

In Jamming, intruder initially keeps tracking wireless medium in order to find frequency at which receiver node is receiving signal from the sender. Intruder then transmit signal in such frequency to ensure malfunctioning of reception.

i)Denial of Service (DoS) attack:

The opponents are aimed at disturbing the entire network operations and routing information of ad-hoc network. This type of attack rejects the valid user access to a particular resource.

j) Selfish nodes: In this attack, the selfish node will not exchange the message to other nodes in the network. The services of the network are not supported by this destructive node. This selfish node uses the network for its own benefit to conserve power.

k) Man-in-the-middle attack:

An intruder sniffs the information which is being transmitted between the sender node and the receiver nodes by impersonate the sender to communicate the receiver or by impersonate the receiver to communicate the sender [3].

l) Impersonation:

This is generally the initiatives for majority of the attacks by using false identity such as using fake MAC address or IP address of other node.

m) Fabrication:

This type of attack creates fake routing information and creates routing error messages stating that the neighbor cannot be called.

n) Gray-hole attack:

In this attack, the malicious node refuses to forward certain packets and simply drops them. It has two stages: in the first stage, the misbehaving node advertises itself as a valid route to reach destination. In the second stage, the node drops the intercepted packets using specific match [4],[6].

o) Spoofing attack:

Same as identity theft, the attacker uses the identity of some nodes to receive the messages of other node. By this, the malicious node misguides the other nodes in the network to create path towards itself to receive its packets.

B) Passive attack:

In this, the attacker steals the useful information from the target network which affects the performance of the network without changing the operation of the network.

Passive attacks are as follows,

a)Traffic monitoring:

It is use to identify the communicating events and functional information of not only MANET but also other wireless networks including satellite, cellular and WLAN. It affects from these vulnerabilities to launch further attacks.

b) Eavesdropping:

It is used to obtain the confidentiality information during wireless communication. In this process, the original message might be eavesdropped and the fake message injected into the network.

c) Traffic analysis:

This attack is used to get information on which nodes communicate with each other and how much data is being processed during the communication.

d) Sync flooding:

This is a denial of service attack. An opponent frequently sends connection request until the resources needed for every connection reach a limit or exhausted. Sync flooding creates resource restrictions for the valid nodes.

There are detection and prevention techniques to many of these active and passive attacks, since this paper gives basics of MANET, we have given information only about the attacks.

VII. CONCLUSION

The aim of this paper is to make students understand the newly emerging mobile communication technology MANET, which enable users to communicate without any physical infrastructure regardless of their geographical location. This paper covers all basic concepts of MANET in a simple manner which will help students to learn about this technology easily and we hope it will create interest to them in learning about MANET.

REFERENCES

[1] Jan Suwart, “Wireless Ad-hoc Networks: Limitations, Applications & Challenges” 08 April, 2008.

[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile ad-hoc Networks: Applicatons and Challenges”.

[3] Priyanka Goyal, Sahil Batra, Ajit Singh, “A Literature Review of Security Attacks in Mobile ad-hoc Network” IJCA (0975- 8887) Volume-9, No.12, November 2010.

[4] Priyanka Goyal, Vinti Parmar, Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application” IJCEM, Vol-11, Jan 2011, ISSN (online): 2230-28993.

[5] Dilip Vishwakarma, Deepak Chopra, “An Efficient Attack Detection System for Mobile ad-hoc Network” International Journal of Engineering and Technology (IJEAT) ISSN: 2249-8958, Vol-1, Issue-6, August 2012.

[6] Ashok Desai, "Review paper on Detection and Prevention of Gray hole Attack in MANET" International Journal of Computer Science and Mobile Computing, IJCSMC, vol-2, Issue-5, May 2013, pg. 105-108.

[7] Ankur O. Bang, Prabhakar L.Ramteke, "MANET: History, Challenges and Applications" International journal of Application or Innovation in Engineering and Management, vol-2, Issue-9, September 2013, ISSN 2319-4847.

[8] Aniruddha Bhattacharya, Arnab Banerjee, Dipayan Bose, Himadri Nath Saha, Deepika Bhattacharya, "Different types of attacks in Mobile ad-hoc network: Prevention and mitigation techniques".

[9] Dhruvi Marsonia, Prof. Hardik Patel, " A Review paper on Network layer attacks in MANETs", International Journal for Scientific Research & Development, vol-1, Issue-9, 2013, ISSN (online)- 2321-0613.

[10] Muhammad Imran, Farrukh Aslam Khan, Tauseef Jamal, Muhammad Hanif Durad, "Analysis of Detection Features of Wormhole Attacks in MANETS" International Workshop on Cyber Security and digital Investigation (CSDI 2015).

[11] Anamika Pareek, Mayank Sharma, "Detection and Prevention of Sybil Attack in MANET using MAC address" International Journal of Computer Applications (0975-8887) vol-122, no. 21, July 2015.