RA Journal of Applied Research
||Volume||1||Issue||1||Pages-8-12||Feb. -2015|| ISSN (e): Applied
www.rajournals.in

Different Types of Security Attacks & Their Counter Measures In Mantes

Authors
Dr. Ajay Vikram Singh[1], Stuti Rikhye[2]
[1]Assistant Professor
[2]MCA Student
Amity University, Noida
Email-avsingh@amity.edu, srikhye@yahoo.com

ABSTRACT :

A mobile node is necessary with a transreceiver which is wireless and permit it to communicate with other node in its radio communication range In this paper , we survey various important security solution for the Mobile Adhoc Network. A Mobile Adhoc Network (Manets) is a dynamic and decentralized type of wireless network always establish naturally by a collection of nodes without help of a permanent infrastructure. Due to dynamic topology , backbone less nature and distributed cooperation of manet make it vulnerable to various security attacks some of the security attacks are black hole attack , neighborhood attack , rushing attack and DOS attack .

***Keywords** :Manets, Secure Routing ,Types of Attacks , Counter measures.*

I. INTRODUCTION :

Adhoc is a wireless network. Each device independently to move in any direction and will therefore , change its links to other device immediately . Security is a mandatory in providing excellent adhoc network . There are various attack which likely to be occur in Manets are black hole , wormhole and rushing attack . The major goal of Manets is to provide various services such as confidentially , timelines and lightweight consumptions, authentication , availability ,integrity

Confidentiality :

It ensures that secrets information's and data is never disclose and keep information sent unreadable to unauthorized devices. . One way to keep information confidential is to encrypt the data and other technique is to use directional antennas . Manets uses an dynamic and open medium , so usually all devices with in the direct transmissions range can obtain the data .It ensure that the transfer data only used by the intended receiver.

Integrity :

In this , received message is not corrupted and ensure that the data has been not altered during transmission .Guarantee of originality means what has been received is exactly same , to whatever was sent .

Availability :

It permits the survivability of network services despite of Denial Of Service attack . It ensure that the adhoc network security listed above are available to the deliberate parties when required . The availability is occur when there is a redundancy and physical protection [2] .

Timeliness :

Packets particularly routing update packets must be reach in defined time span.

Lightweight Consumptions :

Routing protocols must have less processing overheads , specially required in MANETS as power or battery consumptions is critical issues .

II. LITERATURE REVIEW :

Two approach in protecting Mobile Adhoc Network are Proactive and Reactive approach .We definitely have to consider the following issues :

Secure Multitasking

Secure Routing

Private Aware Routing

Key Management

Intrusion Detection System

Multichip

Wiretapping

Some of the efficient routing protocol are DSR(Dynamic source routing). Adhoc on demand vector routing. A source driven ,loop free and efficient routing protocols is an DSR. some of the major constraint or parameter , which are required by users as QOS guarantee are bandwidth , end-to-end delay , jitter ,probability of power loss.

III . VULNERABILITIES OF MANETS :

Vulnerability in Manet is a weak point in security system. Manet is vulnerable but not wired. There are several vulnerabilities are as follows [2] :

No predefined boundary :

In Mobile Adhoc Network , we can't explain about a boundary of a network .They work in a enivornment which is nomadic where they allow to join and leave wireless network .As soon as some adversary come into range of a node it will be able to communicate with that node . The protection includes in this are impersonation , Denial of service attack (DOS) and replay .

Resource Availability :

of self organized security mechanism. Resource availability is important issue in MANETS. Protections against specific threats. Adhoc environment also allow implementation

Adversary inside a network :

The Manets nodes are free to move and leave the network because it create dynamic topology . The node within a network may also behave selfish node . Thus , this attack cause harm than outside attack. These convergence are called comprised convergence .

Table 1 . Attacks on different layer :

Layers	Attacks
Multilayer	DOS , Impersonation , Replay.
Physical layer	Jamming, interception ,Eavesdropping
Data link layer	Traffic analysis , Monitoring .
Network layer	Wormhole, Black hole , Byzantine
Transport layer	Hijacking Flooding
Application layer	Corruption of data ,Repudiation.

At different layers of OSI model implemented in MANETs there are different attacks and vulnerabilities. Start from Application layers where some of the major attacks are data corruptions and repudiation , transport layers attacks are hijacking flooding , network layer attacks are wormhole ,black hole , byzantine , data link layer attacks are traffic analysis and monitoring , physical layer attacks are eavesdropping , interception , jamming [6]. In multi layer attacks are DOS , Impersonation and Replay [1] .

IV. TYPES OF ATTACKS IN MOBILE ADHOC NETWORK :

In this , we discuss various types of attack in Mantes .The attacks in Mantes classified in to two categories : internal and external .Then we introduce main type of attack which are denial of attacks , eavesdropping attacks , black hole attack , wormhole attack , Neighbor attacks and Rushing attacks . Selective black hole attack is a special kind of black hole attack where false node fall the data packet selectively .There are two kind of black hole attack as follow : single black hole attack and multiple black hole attack . We use IDS (Intrusion Detection System) to detect and report the harmful activity in Adhoc Network [5].

Eavesdropping Attack :

In fig 4.2, Eavesdropping is another kind of attack occur in Mobile Adhoc Network. The goal of eavesdropping is to obtain some confidential information that should kept secret during the communication. This secret information may include the location , public key , private key or even passwords of the node . Because such data are very important to the security states of the nodes , it should be kept away from unauthorized access.

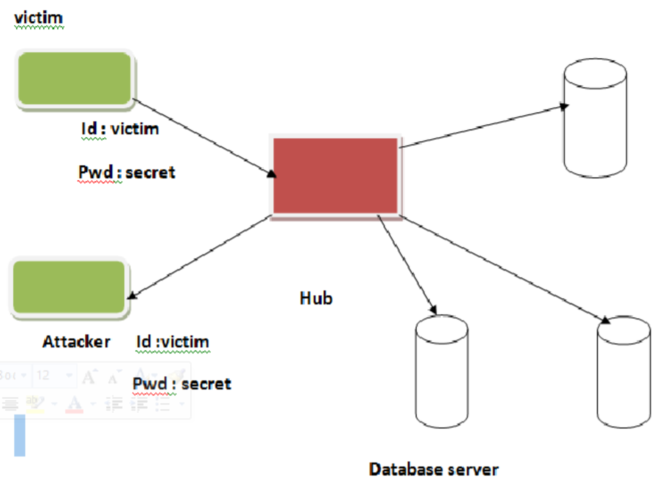

Fig 4.2 Eavesdropping

Flooding Attack :

In fig ,it is also denial service attack .The selfish node may be or may not be part of a Manets , may send huge number of packets to a node which is a part of a network and may disrupt the service of the victim node.

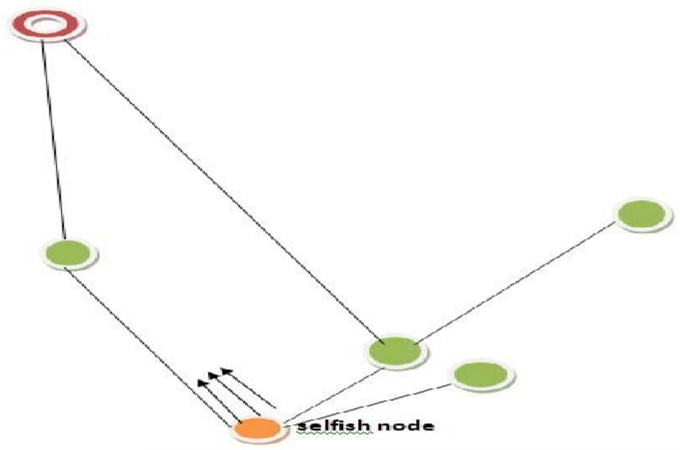

Fig 4.3 flooding attac

Rushing Attack :

In this attack DSR protocol , have to identify duplicate route request packets , each intermediate node discards all duplicate packets (with same request ID) and only process first non duplicate packet . By modifying or skipping some of the routing processes , a rushing attacker can forward these duplicate packets and disrupt routing process[4].

Wormhole Attack :

In this attack , a harmful node receives packets at one position in the network and then dig them to another position in the network , where these packet of data are resent into the network . This tunnel between two colluding attackers is referred to as wormhole .

DOS Attack :

It is next version of jamming attack , this attack is an attempt to make a computer recourses unavailable to intended users . Denial of service attack is an explicit attempt by attacker to prevent valid users of a service from using that service . for example : flooding of network , disrupting service to specific person, need of computational recourses such as bandwidth , disk space or CPU time.

Exploit Attack:

In this type of attack , the attacker knows of a security problem in a piece of software or operating system. It is a modern wireless attack and open network impersonation.

V. COUNTER MEASURES FOR DIFFERENT ATTACK :

Measure of flooding attack :

Attacks can be disrupt by various protocols . The main reason is that all nodes are participating malicious node also and followed by neighbor node ,it the RREQ rate of any neighbor is predefined threshold the node record its information or detail and put it separate .All the RREQ from a separate list are dropped.

Measure of link layer attack :

DSR protocol to protect link layer and network layer CCMP AES mode is used , the main center of this mode is to provide protection while transmitting data packet in a point to another point manner through the security protocol CCMP AES working in data link layer and it keeps data and information frames from eavesdropping etc .

VI. DISCUSSION AND CONCLUSION :

In this survey paper , we discuss about various important security solutions in Mobile Adhoc Network and analyze the main security criteria of Manets . We discuss various vulnerabilities , attack on different layers , most of which are caused by the character tics of Mobile Adhoc Network such as limited battery power , open media , constantly changing topology .There are several attacks that threaten the Mobile Adhoc Network .According to these attacks , we survey security techniques and solve problem in Manets . At the last ,we discuss security measures that can help to protect Manets . In this research paper , we try to explore more points in future .

REFERENCES :

[1] A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks by Bing Wu, Jinmen Chen, Jibe Wu, Michaela Carded .

[2] Security Issues in Mobile Ad Hoc Networks- A Survey by Weenie Li and Anuran Joshi.

[3]Study of various attack in Manets and elaborative discussion of rushing attack nods with clustering scheme by rush nanny.

[4] A survey of black hole attacks in wireless mobile ad hoc networks. Fan-Shun Tseng1, Li-Deer Chou1 and Han-Chief Chao2,3,4*.

[5] DSAB – A hybrid Approach for providing security in manets , Goshen Kumar Roy .