Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

Security Issues and Attacks in Mobile Adhoc Networks

Ms. Rajshree Soni[1]
[1]Scholar,
MTech CSE Mody University of Science & Technology,
Lakshmangarh (Sikar)

Dr. Anil Kumar Dahiya[2]
[2]Head of Department,
CSE Mody University of Science & Technology,
Lakshmangarh (Sikar)

Mr. Sourabh Singh Verma[3]
[3]Assistant Professor,
CSE Mody University of Science & Technology,
Lakshmangarh (Sikar)

***Abstract*: Mobile Ad Hoc Network (MANET) is a dynamically forming network containing multiple wireless mobile nodes. The nodes in MANET are deployed in an environment where no pre-existing infrastructure exists and these nodes are free from any kind of centralized control. Researchers have developed numerous routing protocols for MANET. Mobile Ad Hoc Network (MANET) is provided with some essential tasks containing routing, Packet forwarding, Node discovery, Packet transmission and network supervision etc.**
Since the topology of Mobile Ad Hoc Network (MANET) changes dynamically caused by the node mobility, providing secure routing is the main area of concern. Even though various routing protocols have been proposed by researchers but while implementing these protocols the efficiency and proneness to numerous security attacks are key points of concern. In this paper first the vulnerabilities in mobile adhoc networks have been analyzed, which have constrained it essentially easier to surmount from attacks than the traditional wired network. Then various security issues are discussed and the attacks in mobile adhoc networks have been analyzed. Then the conclusion and future work is discussed.

Keywords: ***MANET, Attacks, Traffic Patterns, Network Behavior***

I INTRODUCTION

Mobile Adhoc Network is an extremely proficient and quick deployable wireless network technology. It is chiefly based on a self structured and shortly used network. MANET is self organized and it means that the data transmission, routing decisions and operations will be carried out by the node itself. MANET is a challenging area of wireless networks. Because of these enormous features, MANET is important to the areas of real world applications where the rapid and unpredictable change in topology occurs [1]. In MANET a node acts as a router and a host in order to transmit data from source node to destination node, and nodes may join and leave the network dynamically because of the node mobility. In this kind of network no centralized control or pre existing infrastructure exists. Mobile Adhoc Networks are greatly prone to various types of security attacks. So it is immensely desirable for MANETs to use secure routing protocols to ensure network confidentiality, integrity, authenticity and availability. A great number of security solutions that works well for wired networks don't fit for mobile adhoc networks. With the use of secure routing protocols, the affect of numerous security attacks can be abridged.

II. REVIEW OF ROUTING PROTOCOLS

A variety of routing protocols are essential for MANETs to globally discover the multi hop routes used to send data packets from one node to another node [2]. In MANET routing protocols are mainly distinguished in two forms: 1. Proactive (Table Driven) 2. Reactive (Source initiated on demand). These routing protocols are categorized as follows:

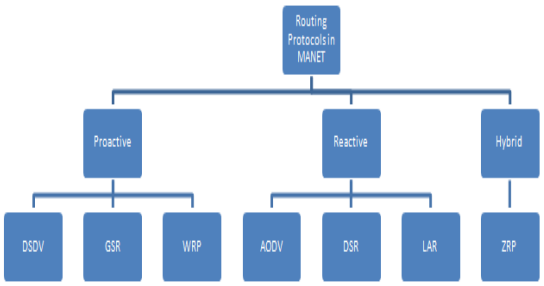

Fig. 1 Routing Protocols in MANET

Most of the researches have been done in MANET taking energy efficiency into consideration**.** a number of the MANET routing protocols are excellent in case of efficiency. However the security needs for these routing protocols altered the situation and a greater detailed study is recently underway to create more secure routing protocols for MANET. These MANET protocols are highly vulnerable to security attacks because of the dynamic topology change. To address these security issues various secure routing protocols have been proposed for example Secure Ad hoc On-Demand Distance Vector Routing (SAODV), Authenticated Routing for Ad hoc Networks (ARAN), Secure Efficient Distance Vector Routing (SEAD) and Secure Routing Protocol (SRP).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

Though researchers have projected numerous secure protocols, their obstruction towards various types of security attacks and quickness are primary connect of approach in implementing such protocols. Hence, there is a crave for review.

III SECURITY ATTACKS IN MANET

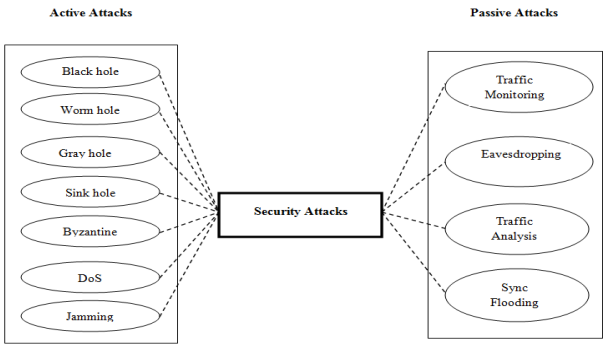

Fig. 2 Types of Security Attacks

Mobile Adhoc Networks are susceptible to several security attacks. The attacks in MANET are classified depending upon diverse unique aspects. In MANET these attacks are primarily classified into active and passive attacks. The major types of attacks that come under these sections are characterized below:

3.1 Passive Attacks

MANETs are highly sensitive to Passive Attacks. Passive Attacks are done with the purpose of stealing the intimate information from the network[3]. The data is not changed within the network if passive attacks are executed but the attackers try to steal the legitimate information by the means of overhearing and traffic analysis. The disclosure of these attacks is difficult because the network operations are not affected. To prevent these attacks highly encrypted data is transmitted over the network.

3.2 Active Attacks

The Active Attacks are very adverse and harmful for a network. The attacker attempts to stop the flow of messages between nodes in the network by the means of active attacks. These attacks help the attackers to make illegal use of the network privileges and so can create congestion, DoS and control packet modification etc. Several security mechanisms are being taken care to deal with this kind of attacks [4].Some of the active and passive attacks are reviewed here.

3.3 Types of Active Attacks

3.3.1 Black hole Attack

In this type of attack, an advertisement with zero metric is sent to all the neighboring destinations by the attacker. The malicious node creates an illusion of having the optimum route to the target node for interrupting its packets. When the route reply is received by this malicious node it sends a forged reply with excessively short route. As soon as the malicious node becomes active it starts interrupting the packets passing between nodes. These sort of attacks are executed at the network layer.

3.3.2 Worm hole Attack

In this type of attack, a tunnel is formed between malicious nodes. Whenever a corrupted node receives a data packet it tunnels this packet to another attacker's node. The tunnel formed between these malicious nodes is called wormhole. Wormhole attack is a rigid threat to the security of MANET routing. This attack prevents the route discovery except the wormhole in protocols like DSR, AODV etc. This attack is normally done at the network layer. Worm hole attack is also executed at the network layer.

3.3.3 Gray hole Attack

This type of attack is basically a malfunctioning of routing mechanisms that result in the communication failure. It includes two stages. First stage includes the node marketing which tells that it has a valid route to destination. Second stage includes node interception with packets exhibiting a specific match[5].

3.3.4 Byzantine attack

This attack includes a set of nodes arranged properly inside a network which work safely and may form attacks by creating routing loops for forwarding data packets through non-optimal routes or arbitrarily dropping packets this causes the interruption of routing services in a network[6].

3.3.5 Sink hole Attack

In this type of attack a sink node is created by the attacker which tries to import the data of the whole neighboring nodes to its sink. This attacking node tries to prepare a very tempting link. Thus, a large amount of traffic reaches to this node. And also the data being transferred between neighboring nodes is overheard by it [7].

3.3.6 Denial of service (DoS) attack

This attack includes making routing services unavailable to the nodes. This attack disturbs the network functioning's including no hitch with security threats [5].

3.3.7 Jamming

Jamming is a sort of DoS attack in which the invader examines the frequency of communication. In this the attacker attempts to jam the network by sending the signal on examined frequency with the intent of blocking the reception of useful packets [8]. These types of attacks are done at the physical layer.

3.4 Types of Passive Attacks

3.4.1 Traffic Monitoring

In Traffic Monitoring the attacker makes use of both data and traffic patterns to carry out the attacks. Since the attacker analyses the traffic patterns, so can steal the intimate data of network topology [7]. The analysis of traffic in the network may lead to the following types of disclosure of the legitimate information:

1. Node location
2. The topology of the network
3. Every node's role
4. Information about the source and destination nodes

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 12, December-2016

3.4.2 Eavesdropping

The term eavesdropping means overhearing the legitimate information without the knowledge of the owner. This type of attack includes the spoofing of conversation or studying the useful information by unintended user. It harms the transmission by eavesdropping the conversation and injecting the forged stream of messages into the network [5]. The main goal of this type attack is to steal the confidential information which might include the private and public key etc. These types of attacks are performed at the physical layer.

3.4.3 Traffic Analysis

Traffic analysis includes inspecting each and every node for getting the information about those nodes whose information may be useful. The attacker also monitors the traffic patterns to figure out the nature of the network.

3.4.4 Sync flooding

Sync flooding is a sort of denial of service (DoS) attack. Sync flooding is done by creating a great number of TCP connections with nodes. This attack creates a severe restriction for valid nodes. These types of attacks are executed at the transport layer.

IV SECURITY CHALLENGES IN MANET

In MANET several security challenges have been taken care into consideration. These challenges are listed below:

- Availability
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation
- Anonymity
- Authorization

4.1 Availability

It demonstrates that the useful resources are provided to the certified users at the time when they need them. Both the data and the services are accessible by the parties. It assures the network survivability even if the exists Denial of Service (DoS) attack.

4.2 Confidentiality

Confidentiality ensures the authorization; it means the legitimate information will be available to only authorized user. Thus in order to ensure the confidentiality of legitimate information or data we need to make sure that only the privileged users access them[9].

4.3 Integrity

Integrity of a message ensures that a message can only be modified by the authorized user. Integrity ensures the identity of a message at the time of transmission. The integrity might be lost in two main ways:

1. Replication
2. Modification of messages

Integrity is compromised by modification of messages by unauthorized users, removing a stream of data or unnecessarily coping of data by the attacker.

4.4 Authentication

Authentication ensures that a node is supposed to respond to only those messages that are arriving from a legitimate node of the network[10]. Thus for keeping the network safe from the security attacks it is essential to authenticate each and every sender of data stream.

4.5 Non-Repudiation

Non-Repudiation ensures the originator and recipient of message and whenever the identification or survey of a node is performed the sender of the message must not deny of having transmitted the message.

4.6 Privacy

Privacy is maintained to keep the legitimate information safe from unauthorized disclosure.

V CONCLUSION

MANET possess dynamic infrastructure and has no centralized control which makes such networks more prone to security attacks. The discussion about different routing protocols in MANET, security attacks and various security challenges have been suggested in this paper. Security attacks that are classified into active and passive types are reviewed here. The major area of concern is to present protected routes in presence of attacks, to perform so techniques using neighboring node's information are being acquired.

REFERENCES

[1] M.M.Alani, (2014, Nov) "MANET security: A survey", In International conference on Control System, Computing and Engineering (ICCSCE'14) IEEE pp. 559-564.

[2] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc Networks: Requirements and Security Management Perspective, Journal of Computer Science and Data Mining ,Vol. 1,No. 1-2,December 2011

[3] Sapna, Gambhir, Saurabh Sharma," PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs", 2013, 3rd IEEE International Advance Computing Conference (IACC).

[4] Ashish kumar khare1, Dr. R. C. Jain2 and Dr. J. L. Rana3" A REVIEW: TRUST, ATTACKS AND SECURITYCHALLENGES IN MANET" Informatics Engineering, an International Journal (IEIJ), Vol.3, No.3, September 2015.

[5] Gagandeep, Aashima, Pawan Kumar, (2012, June)"Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Vol.1, No.5.

[6] YIH-CHUN HU, ADRIAN PERRIG and DAVID B.JOHNSON (2005, NOV) "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks, Springer Science.

[7] Reijo M. Savola and HabtamuAbie (2009, Sep) "On-Line and Off-Line Security Measurement Framework for Mobile Ad Hoc Networks" Journal of Networks, pp. 65-379, Vol.4, No.7.

[8] C.Sreedhar, Varun Verma Sangaraju, (2013, Oct) "A Survey On Security issue IN Routing IN MANETS", In International Journal of Computer Organization Trends Volume 3 Issue 9(IJCOT) pp. 399-406.

[9] Wenjia Li and Anupam Joshi "Security Issues in Mobile Ad Hoc Networks - A Survey" Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.

[10] Mohammed Saeed Al-kahtani, "Surve y on Security Attacks in Vehicular Ad hoc Networks (VANETs)," IEEE 2012