International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 1 (February '2017)
Special Issue on 1st National Conference on Advanced Computing and Communication Technologies,
Conference held at Siri PSG Arts and Science College for Women, Sankari,Tamilnadu,India.

MOBILE AD-HOC NETWORKS: SECURITY ATTACKS

J.Selwyn Paul ,
Computer Science Department,
St Joseph's College,
Bengaluru, Karnataka,India.

D.Ravi Kumar,
Computer Science Department,
St Joseph's College,
Bengaluru, Karnataka,India.

Abstract: Mobile ad-hoc network is a very interesting research area. A mobile ad-hoc network consists of nodes which can move freely. There are intermediate nodes which can communicate between channels. The techniques used in MANET open peer –to-peer network architecture, wireless mediums, network topology. Security challenges have to look into primary concern to provide secure communication. This paper we discuss the various security issues, threats and different measures to handle them.

Keywords : Mobile Ad-hoc Network,FSR, GPSR, Detection of Intrusion, DOS.

I.INTRODUCTION

In mobile technology, there are two main technique which access wireless interface between the hosts. Firstly, enabling cellular structure to carry data and even voice which includes major concern. Secondly, communication takes place between users of ad-hoc networking. Packets are given from source to destination, so that the information will be transferred. MANET very useful compared to cellular network. Mobile network, where each and every device move frees as a single unit in any of the direction & changing the links to another device offend. Ad-hoc network doesn't depend on any pre defined structure. Therefore they can bring into effective action without placing on any of the structure. It uses in situations very difficult situation. MANET might be liable when we check to wired network. Security based issues in internet technique may attack connectives of internet and it attacks ad hoc routing protocol.

Evolution of MANET

In the year 1970, Normal and his researches at the university of Hawaii invention of ALOHA net.
In the year 1972, Packet Radio Network.
In the year 1980 Survivable Radio Network and Internet Emerging Task force, is termed as mobile ad hoc group of network. .

A MANET is a collection of wireless nodes from mobile nodes, whether it can be temporary/ short lived network where all nodes are free to move and configure themselves. In the concept of MANET,we have nodes that connects both host and router , even in the case of topology there is changes in networked used in it .

Different types of routing and network technique used MANET

1. Uni-casting Routing
2. Multi cast Routing
3. Dynamic topology.
4. Rate
5. Network over headed.
6. Scalable
7. Routing
8. Service of quality [2].

II. ROUTING CLASSIFICATION PROTOCOLS IN MANET'S

Classification of routing protocols in MANET's can be done in many ways. According tothe routing strategy the routing protocols can be categorized as source initiated, depending on the structure of network classified various routing classification as flat routing, hierarchical routing and geographic routing.

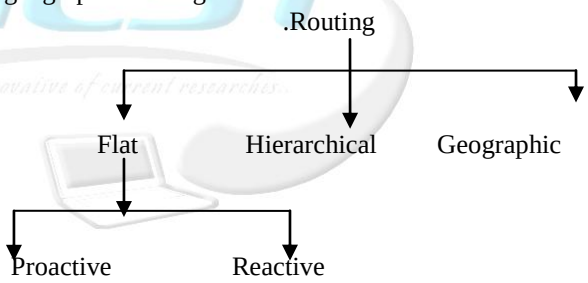

Fig: Classification of Routing in MANET Networks.

Flat routing

Routinginformation to routers that are connected to each other without any organization or segmentation structure between them.

Flat routing protocol is further divided into two different types.

1. Proactive
2. Reactive

Proactive: These protocols are also called as proactive protocols since they maintain the routing information even before it is needed .Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. There exist some differences between the protocols that come under this category depending on the routing

information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. In proactive method the network which is large, have difficulties in using the node from routing table. Therefore overhead in routing table have more bandwidth.

Different types of Proactive

- FSR (Fisheye State Routing)
- FSLS(Fuzzy Sighted Link State)
- OLSR (Optimized Link State Routing)
- TBRPF (Topology Broadcast Based on Reverse Path Forwarding)

Reactive: These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there not at all communication. If any nodes want to communicate a packet of information from one node to other node then the protocol will have the connectivity established in order to emit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network[2][3].

Hierarchical routing

In this type of routing technique that have hierarchic in different nodes that resides over. In proactively approach the routers and then serves the additional active nodes create lower levels in reactive flooding. Hierarchical routing method have different choices to be made to get levels of choices by the method.

Examples of hierarchical routing method.

1. Cluster based Routing protocol.
2. Fisheye State Routing Protocol.
3. Hierarchical Link State Routing Protocol based on Zone.

Geographic Position Information Assisted Routing

Geographic routing requires that each node can determine its own location and that the source is aware of the location of the destination.

- LAR (Location-Aided Routing)
- DREAM (Distance Routing Effect Algorithm for Mobility)
- GPSR (Greedy Perimeter Stateless Routing)

Broadcasting techniques

1. Unicasting: It is defined as a broadcasting process where the information is send from the source to a single destination.
2. Multicasting: It is defined as a broadcasting process where the information is send from a source to asset of destinations.
3. Broadcasting: It is defined as a broadcasting process where the messages are flooded from a source to all other nodes in the specified networks.
4. Geocasting: It is the process of sending of information from the source to all other nodes inside a geographical region.

III. SECURITY FACTORS INVOLVING IN MANET

Susceptibility is very weak in the aspect of security. System can unsafe because the system does not check the user's identity before accessing the data. MANET is very vulnerable than wired network.

Listed out are the vulnerabilities:

1. **Lack of centralized management:** MANET does not centralize monitor server. The absence of centralized management more attacks difficult so that monitoring the traffic in a large scale network. Lack of centralized management can destroy the nodes.
2. **Availability of Resources:** Availability of a resource is an important issue in MANET. Providing unthreatened communication in such environment against particular threads and attack, leading to various security issues and architecture. Collaborative ad- hoc environment allow us to have organized security mechanism [4].
3. **Scalability:** Nature of nodes which is used in mobile and ad-hoc network changing every time frequently. So that scalability is the issue with security. Security techniques should be capable of accessing various large and smaller networks.
4. **Cooperativeness:** Routing algorithm for MANET usually nodes are cooperative andvicious. As a result harmful attackers can easily attack and disobey the protocol specification of network.
5. **Dynamic topology:** Dynamic topology and changing of nodes may disturb the involvement of trust build among the nodes. This dynamic topology can be protected with distributed and adaptively looking in the different area of security measures.
6. **Limited power supply:** The nodes in MANET have to consider the confined power supply. In MANET there is only a limited power of source, so it makes use of itself. By consuming the large amount of battery,which in turn ties to decrease the performance of networks from different attackers.
7. **No pre defining boundaries**:In the mobile ad-hoc network the wireless technique, the nodes which leave whenever required and join the wireless network. Wireless network will communicate with nodes in radio range.
8. **Adversary inside the Network:** the mobile nodes within the network can leave a network. The node within network may also behave maliciously.Therefore this attack is more dangerous than external attack.
9. **Bandwidth constraint:** Low capacity links may exist to wireless network which are more Variable low capacity links are susceptible to external noise and interference.
10. **No predefined Boundary:** In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The attacks include Eavesdropping impersonation, tempering, replay and Denial of Service (DoS) attack.[5]

IV.ATTACKS CLASSIFICATION

1. Attacker behaviors

There are two kinds of attackers namely passive and active attackers.

- Passive attacks are listens which target the networks.In this technique, the attacks listen to network to get data about what exactly is happening in the network.
- In active attack the attackers disturbs the performance of the network, it take the important information and tries to destroy the date while the network is been exchange. Active attacks could be external are internal attack. Active attacks include Data modification by Viruses and Trojans.

2. The origin of attacks

The origin of attackers are classified into two external and internal

- External attacks are launched by users who are not authorized to communicate in the network operations. These attacks mainly caused due to congestion of network and denial of access to specific network function, so that the whole network operation is disrupted
- Internal attacks are done by authorized nodes in the network, and misbehaving of nodes. If the external nodes are kidnapped the authorized internal nodes are then attacks against the ad-hoc networks[6].

3. **Capability of Attackers**.

The capabilities of attackers are in two ways we compare between Mobile and Wired.

- Mobile attackers have the capabilities as any other node in network of ad hoc. Because of usage of battery and capabilities. Mobile attackers jam the wireless.
- Wired attackers that are accepting access to the external resources, since more resources several attacks will be taken place in the network as such that the complete network can be jammed.

4. Attackers Number

The number of attackers are differentiated in two ways primarily Single Attackers and Multiple attackers.

- Due to longer reach and wired facilities the traffic of attackers is wide to reach any wired facilities. Therefore they have very resources that have been a weak point to them.
- Colluding attackers should easily shut down the singly node in the network and effectiveness of network distributed operation involving security.

V. APPROACHES TO DETECT THE HARMFUL NODES IN THE NETWORK.

- **ACKNOWLEGMENT :** In this approach 2 acknowledgement packet in opposite direction of path of routing. Due to which data packets are received.
- **BEST FAULT TOLERATE ROUTING :** In this approach the acknowledgement which has to be send from destination to destination to check the quality of destination node from the monitor.
- **CBCS :** In this approach the mechanism of DSR which detect harmful nodes in network.it combines both the advantage of proactive and reactive schemes to detect harmful node
- **INSTRUSION DETECTION :**Node in the MANET participates in the process sends the information to other nodes in the network. LEE proposed this approach, to have distributed and frame work to detect the attack. [7].
- **CLUSTER BASED INTRUSION DTECTION:** In the approach the complete network will been made us clusters so that one node member is member of one or more clusters.
- **DEFENDING WORM HOLE ATTACK :** Wormhole attackers will defends the usage of packets. This will provide maximum transmission distance that will be packet to maximum information. Receiver checks for time complexity and distance of transmission.

VI.CONCULSION

MANETs, the most spoken term in wireless technologies, approach to be the ruler of future airs provided the vision of anytime, anywhere communications In this paper we, introspect the various security measures of the Mobile Ad hoc network. Primarily in this paper we introduced the security issues that relates MANETs. Secondly the paper ends with the different approaches which detects harmful nodes in the MANETs.

VII.REFERENCES

[1]. S.-J. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia, 2000: "A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols," In Proceedings of IEEE INFOCOM 2000, pp. 565–574.

[2]. Changling Liu and Jorg Kaiser.2005: "A Survey of Mobile ad hoc network routing protocols", University of Ulm Tech. Report Series.Wu., 2002: "Mobile ad hoc networks and Routing Protocols" Handbook of wireless networks and mobile computing,pp.371-392

[3]. Banta Sigh. & Manish Kumar "Study on Security Issues & Challenges in MANET","PARIPEX - INDIAN JOURNAL OF RESEARCH", Volume: 3, Issue: 4,April 2014, pp. 54-57.

[4]. Chang Li Shi, Lan Yang Hao, Sheng Zhu Qing (College of Computer Science Chongqing University Chongqing, China). *Research on MANET Security Architecture design*.

[5]. Joshi Nikhil R, D.N Chandrappa,"MANET *Security Based On Hybrid Routing Protocol and Unique Cryptographic Identity"*

[6]. KhalaBabak Hossein, BagheriHamidreza, Katz Marcos, Salehi Mohammad Javad, mohammadpour Mohammad Noor, and AsghariPariSeyed Mohammad. *A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks.*