ISSN: 2321-7782 (Online)
Volume 3, Issue 8, August 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

# Mobile Ad-Hoc Network (MANET) and its Security Aspects

**Ku. Vishakha V. Vyas**[1]
Department of Computer Science & Engg.
Anuradha Engg. College,Chikhli.
Maharashtra, INDIA

**Nitin K.Bhil**[2]
Professor, Department of Computer Science & Engg.
Anuradha Engg. College,Chikhli
Maharashtra, INDIA

***Abstract: Mobile ad-hoc network becomes a centre of attraction in technological area now-a-days. Mobile ad-hoc network (MANET) is a "infrastructure-less" network and hence can work in slow network area also. The node can communicate directly with other node available in network or can use mediator nodes to makes communication between source and destination. This paper deals with different routing protocols and issues of MANET. Also this paper includes security aspects of MANET, which is quite important to discuss about because MANET having dynamic topology and affected by lots of security threats.***

***Keywords: mobile ad-hoc network; routing protocol; security aspect; topology.***

## I. INTRODUCTION

Wireless ad-hoc network is a point-to-point network or we can called it as 'peer-to-peer' network, which is now-a-days become a centre of attraction in corporate and research area. The word "ad-hoc" is a Latin word and stands for "for this purpose". Wireless ad-hoc network is formed from node to node, where each node acts as a host as well as router at the same time. This type of network can be used when there is requirement for short period communication or in such areas where wired connections are failed. A wireless ad-hoc network is divided into three main types: Wireless sensor network (WSN), Wireless mesh network (WMN) and Mobile ad-hoc network (MANET). A "Wireless sensor network" is a communication network where sensors are used which acts as nodes. For example, VANET i.e. vehicular ad-hoc network which uses sensor in vehicles. The sensor can predict the surrounding vehicles and notify the driver about them. This system is helpful in reducing accidents. A "wireless mesh network" is a communications network made up of radio nodes arranged in a mesh topology. For example, the laptops in the One Laptop per Child program use wireless mesh networking to enable students to exchange files and get on the Internet even though they lack wired or cell phone or other physical connections in their area[3].

Mobile ad-hoc network (MANET) is a "infrastructure-less" network and having a "dynamic topology". As mobiles are portable device, it can be moved from networked area to non-networked area. If there were no any network, no two devices establish connection with each other. So, in these types of cases mobile ad-hoc networks are used. The mobile device or node can communicate directly with other device available in network or can use mediator nodes to makes communication between source and destination. As MANET's topology is dynamic in nature, it is affected from lots of security threats. There are three types of MANET; Intelligent Vehicular Ad hoc Networks (InVANETs), Internet Based Mobile Ad hock Networks (iMANET) and Vehicular Ad hoc Networks (VANETs). Consider a simple example to better understand the concept of mobile ad-hoc network. Consider three nodes(S, A, L). Suppose node A want to communicate with node L and node L is in the network of node A, so they can communicate directly. Now consider node S want to communicate with node L, but they cannot communicate directly as there is no network. So, now the node S sends packets to node A which works as a mediator between node S and L as it comes in the network of both the node S and node L. Now the node A transmits the packets to node L, and in this way the packets are travels from source to destination using ad-hoc network.

 

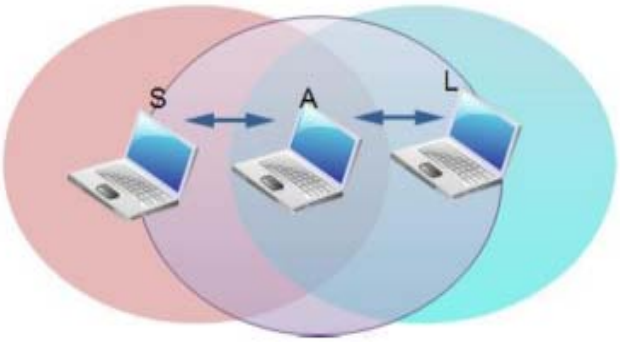


*Fig 1: An infrastructure-less network (MANET) [7]*

## II. ROUTING PROTOCOLS USED IN MANET

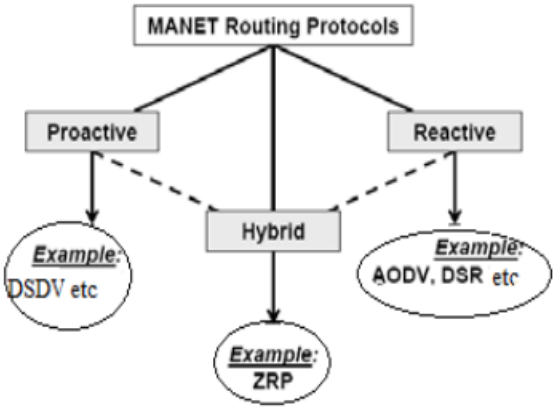


*Fig 2: Types of routing protocol in MANET [1]*

### *A. Proactive routing protocol*

Proactive routing protocol is also known as "table-driven routing protocol". In table driven routing protocol as name indicates, each node has to maintain one or more tables to store the routing information. This table is maintained throughout the network so as to maintain consistency of its view. As we know MANET having dynamic topology and it continuously changes all time, so each node has to update the table to maintain the consistency of network view. In proactive routing protocol, if there is no connection or communication between two nodes, still they have to maintain their table and it's updation. Some types of proactive routing protocols are Destination sequenced distance vector (DSDV)[4], WRP, GSR, FSR. One of the most popular proactive routing protocols is Destination sequenced distance vector.

### *B. Reactive routing protocol*

Reactive routing protocol is also known as "on-demand routing protocol". In reactive routing protocol, there is no need to maintain the routing table at each node. Instead, if any two nodes want to communicate with each other or any node want to send packet to another node, then this reactive routing protocol searches for the route and establish the connection between the nodes. After establishing a good connection, they can quickly transmit and receive data packets. Some types of reactive routing protocols are Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), CBRP. One of the most popular reactive routing protocols is the Ad hoc On-Demand Vector (AODV) routing protocol. AODV is a reactive routing protocol, discovering routes only when they are needed. "It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within ad hoc network" [6][8].

 

### C. *Hybrid routing protocol*

Hybrid routing protocol is a combination of proactive routing protocol and reactive routing protocol. In hybrid routing protocol, firstly node identify the route using the proactive routing protocol and then later uses reactive routing protocol. Depending upon the different network scenarios, both pro-active and reactive nature of the protocol can be used interchangeably. Some types of hybrid routing protocol are Zone Routing Protocol (ZRP), Zone-Based Hierarchical Link State (ZHLS). One of the most popular hybrid routing protocols is Zone Routing protocol. The basic operation of Zone routing protocol [10] is, it uses proactive routing algorithm within the given zone and reactive routing algorithm outside the zone as defined by user.

## III. ISSUES IN MANET

*A.* Network topology changes many times and not predictable i.e. having dynamic topology.

*B.* Low channel access because of variation in different bandwidth i.e. having low bandwidth optimization.

*C.* Expose station and Hidden station problem.

*D.* Many times it happened that more access link will be same.

*E.* Lack of centralized System/Entity.

*F.* Limited power supply.

## IV. SECURITY ASPECTS IN MANET

### 1) *Security attacks*

» **Passive attacks:** Passive attacks are silent but most dangerous as it silently monitors victim's data without altering it. And hence detection of passive attacks is very difficult since the operation of the network itself does not get affected. Some of the passive attacks are as shown below:

- Snooping: Snooping is one of the passive attacks whose goal is to just monitor the activity of two communicators or networks without altering any data. It includes observation of confidential emails or chats.
- Eavesdropping: Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. Eavesdropping is quite similar to snooping attack. The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication by simply monitoring it. The confidential information may include the location, public key, private key or even passwords.
- Traffic analysis: Traffic analysis is also a passive attack whose name itself indicate its work, it analyses the traffic pattern of the network. So the opponent steals confidential information about network topology simply by analyzing the traffic of network.

» **Active attacks:** Active attacks are either external or internal. Active external attacks can be carried out by external source which do not belong to network while the active internal attacks are carried out by malicious node present inside the network. Active internal attacks are more severe and hard to detect as it present inside the network.

- ***Network layer attack: Some of the different types of attacks on network layer are given below***:

o Worm-hole attack:

The worm hole attack [5] is harder to detect as it does not make any changes in network, instead it slowdown the operation. The worm-hole attack uses "tunnels" to send the data packet from one point to another. Suppose source node want to send data packets toward the destination node. Firstly, source node sends RREQ (route request) message which passes through all the nodes present between source and destination. Let two of the middle nodes are affected or they are malicious nodes. When

 

RREQ message is received by first affected node, it sends that message toward its neighboring malicious node. Tunnel is available between these two malicious nodes which is known as worm-hole. Then it sends RREP (route reply) message back to source and source sends all the data packets through that path, considering that this is the shortest path to destination. All the data packets are passes through the malicious nodes and takes maximum time to reach toward the destination. Hence, results in late packet delivery.

- Black-hole attack:

The black hole attack works same as the concept of "black hole" in space. When the packets arrive towards the node, it absorbs that packet without forwarding it towards the destination. When source sends RREQ (route request) message towards the destination, it travels through all nodes available between the source and destination. If one of the middle nodes is affected by black hole attack, it receives the RREQ and sends RREP (route reply) message back to source indicating that there is short path available from that node for destination. Once the RREP is receive by the source, source sends all the packets toward that affected node and packets gets discarded by that node. Due to this, congestion occurs in network and hence slowdown the network [9].

- Routing attack:

Routing protocols are one of the most important part of mobile ad-hoc network and hence several attacks are mounted on it. The attacker's aim is to interrupt the proper operation of network using attacks such as Packet Replication, Routing Table Overflow, Route Cache Poisoning, Routing Table Poisoning [2] and so on.

- ***Transport layer attack: Some of the different types of attacks on transport layer are given below:***

- Session hijacking attack:

In session hijacking, attackers exploit the unprotected session once its initial setup is done. Attacker steal the victim node's IP address and finds its correct sequence number and then apply various denial of service (DoS) attacks to it.

- ***Multi layer attack: Some of the different types of attacks on multi layer are given below.***

- Denial of service:

This attack aims to attack the "availability" of a node or the entire network. If the attack is successful the services will not be available and hence the network will not work for longer period.

- Jamming:

After determining the frequency of communication jamming is initiated by malicious node. Jamming is one of the types of denial of service.

- Impersonation:

Impersonation attack aims to attack the "confidentiality" and "authenticity" of a network. The attacker uses to impersonate the address of other user node in order to change the network topology. When source want to send the data packet toward the destination, this malicious node portray the address of destination and acts as destination node. So source sends all the data information towards this malicious node and the data remain no more confidential.

***2) Security goals:***

There are 5 main security goals are provided for MANET which are as explained below:

» Availability: Availability ensures the permanency of information or the information that is available all the time. This security goal is ensure to protect a network against the attacks such as denial of services.

 

» Confidentiality: Confidentiality means, only the authorized user has the privilege to access certain information. This security goal is ensure to protect a network against the attacks such as eavesdropping and impersonation.

» Integrity: Integrity ensures the completeness of data that means there is no altering of information. This security goal is ensure to protect a network against the attacks such as modification of message.

» Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. This security goal is ensure to protect a network against the attacks such as impersonation.

» Authorization: Authorization ensures that different types of users can have different access rights. This security goal is ensure to protect a network against the attacks such as session hijacking.

## V. CONCLUSION

The aim of this paper is to understand the basic concept of mobile ad-hoc networking along with its security aspects. As mobile ad-hoc network becoming widest area of research, lots of modifications are occurring day-by-day. As routing protocol is key concept in MANET, security solutions for this is researcher's main aim. The issues and security attacks mentioned above in paper is development topic for researcher's.

## References

1. Aarti, Dr. S. S. Tyagi, " Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
2. Abhay Kumar Rai,Rajiv Ranjan Tewari,Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", nternational Journal of Computer Science and Security (IJCSS), Volume 4, Issue 4, Pages 265-274, Year 2010.
3. Vanita Rani , Dr. Renu Dhir, "A Study of Ad-Hoc Network: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.
4. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", In Proceedings of ACM SIGCOMM, pages 234-244, 1994.
5. Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks".
6. Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", IEEE International Conference on Telecommunications and Malaysia International Conference on Communications,2007.
7. Saleh Ali K.Al-Omari1, Putra Sumari2, "An overview of Mobile Ad Hoc Networks For The Existing Protocols And Applications", International journal on application of graph theory in wireless ad hoc networks and sensor networks(Graph-Hoc), Vol.2,No.1,March 2010.
8. Perkins C., Belding-Royer E., Das S., "RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing", http://www.ietf.org/rfc/rfc3561.txt, 2003.
9. M.A. Shurman, S.M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, pp. 96-97, 2004.
10. Siddhu Warrier, " Characterisation and Applications of MANET Routing Algorithms in Wireless Sensor Networks", Master of Science School of Informatics, University of Edinburgh, 2007.

 