An Exploration of Mobile Ad hoc Networks

Ridhi Chawla[1] (Student) Department of Computer Science & Engineering, Kurukshetra University.SIET Aliyaspur,Haryana, India,
Pankaj Kapoor[2](Asstt. Prof.), Department of Computer Science & Engineering. Kurukshetra University.SIET Aliyaspur,Haryana, India.

Abstract: A Mobile Ad Hoc network(MANET) belongs to the infrastructure less category of wireless networks. It is a collection of nodes which are mobile in nature and transmit data to each other. These mobile nodes move independently, themselves act as routers and take part in the discovery of the routes and their maintenance. MANET works with wide range of protocols which are Table Driven, On-Demand and combination of both the Table Driven and On-Demand protocols. Security of the MANET is an important concern because of its characteristics such as actively changing topology, frequent motion of nodes that act as routers in the network. Various kinds of attacks effect the security of MANET and these attacks needs to be discovered and mitigated. We examine in this Paper the important features of the MANET such as Types of MANET, Routing Protocols, Various Applications of MANET, the problems of Security in MANET.

Index Terms:MANET, PRNET, SURAN, VANET, InVANET iMANET

1.INTRODUCTION

1.1 *History Of MANET*

MANET(Mobile Ad hoc Network) can be categorized into three generations. The MANETs which we are using today belong to the third generation. The first generation came into existence in 1972 and were known by the name PRNET(Packet Radio Networks). Later in 1980's PRNET evolved as SURAN (Survival Adaptive Radio Networks).PRNET were used in combination with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access) for medium access control at data link layer. During that time PRNET were used temporarily in order to provide different networking facilities in a typical environment.

Later in 1980s came second generation of ad-hoc networks,at that time the ad-hoc network systems were further modified and worked as a part of the SURAN (Survivable Adaptive Radio Networks) program. This lead to the Infrastructure less environment for packet switched network. This program helped a lot in improving the performance of the radio signals by making them much smaller, cheaper, and flexible to electronic attacks. Then further in the 1990s, the concept of promotional ad-hoc networks came into being with note-book computers and other possible communication devices. In addition to this , the idea of a combination of mobile nodes was proposed at various research conferences. A lot of work was performed and success was achieved for Ad Hoc Standards upto mid 1990s. With the help of IETF (Internet Engineering Task Force), the MANET group was formed that worked in a manner to standardize routing protocols for ad hoc networks. At the same time while MANET group was making efforts to standardize the protocols on the other side the IEEE 802.11 subcommittee standardized a medium access protocol that was based on the concept of collision avoidance and hidden terminals, to generate prototypes for mobile ad hoc network with the help of notebooks and 802.11 PCMCIA (Personal Computer Memory Card International Association) cards.

The wireless networks that are active in today's environment can be classified into two classes. The *first class* is called as infrastructure based networks with fixed and wired routers and gateways. Wireless local area networks (WLANs) is the most common example of the wired class. It is "one-hop" network The second *class* of mobile wireless network is the infrastructure less mobile network, known as the MANET(Mobile Ad Hoc Network). MANET is usually a "multi-hop" network which does not require any fixed infrastructure. In this type of network the nodes are mobile and independent and does not depend upon any centralized node. These mobile nodes transmit data to each other thus in this way communicate in a network .

1.2 *MANET*

MANET or Mobile Ad hoc Network can be well defined as

Mobile-Free to move and not fixed
Ad hoc- Not planned in advance
Network- An interconnected group or system to carry out the communication.

Security in mobile ad-hoc networks is hard to achieve due to dynamically changing and fully decentralized topology as well as vulnerability and scarcity of

wireless link. Denial of Service (DoS) attack protection and ensuring that packets must not travel through any un-trusted node.[1]. MANETs have a dynamic topology where links are formed and broken with time. These links can be unidirectional or bi-directional .Routing in MANETs involves designing a protocol which helps using routing data packets from source to destination with minimum possible hops and minimum battery power consumption of nodes. The routing protocols for MANETs can be broadly classified into three major categories-Reactive, Proactive and Hybrid[2].

1.3 *Types of MANET*
There are three types of MANETs which are working in present scenerio:

(a) Vehicular Ad-hoc Networks (VANETs)
Vehicular Ad-hoc Networks (VANETs) play a greater role in the communication among the vehicles that act as mobile nodes and between the vehicles and roadside equipment.

(b). Intelligent vehicular ad-hoc networks (InVANETs)
Intelligent vehicular ad-hoc networks (InVANETs) are based on artificial intelligence and specially designed to help the vehicles moving on the road to behave in an intelligent manner during vehicle-to-vehicle collisions, accidents, etc. The main purpose of InVANETs is the road safety.

(c)Internet Based Mobile Ad-hoc Networks(iMANET)
The third type of MANET is Internet Based Mobile Ad-hoc Networks (iMANET) that connect mobile nodes and fixed Internet-gateway nodes. In these type of networks normal ad hoc routing algorithms don't apply directly.

2.CHARACTERISTICS OF MANET

(a)*Self Governing Behaviour*: In MANET, each node act as both host and router. When a source node and destination node is out of the radio range to send or receive any message respectively, at that time the MANETs are capable of multi-hop routing.

(b)*Actively changing Network Topology*: The nodes can join or leave the network anytime, making the network topology dynamic or actively changing in nature.

(c)*Spontaneous Behaviour*: It demands minimum human interference to configure the network.

(d)*Harmonious Environment*: All nodes have indistinguishable attributes with similar responsibilities and capabilities and therefore it leads to complete symmetry and harmony in an environment.

(e)*Centralized Firewall Absent*: Distributed nature of operation for security, routing and host configuration.

(f)*User Density and Mobility*: MANETS provide High user density and large level of user mobility

(g)*Less Memory and Power Usage*: Mobile require less memory,and consume less power and have many light weight features.

(h)*Inferior to Wired Links*: The Stability, Reliability, Efficiency.and capacity of wireless links are lesser than wired links so there is variation in the link bandwidth of wireless links.

3. APPLICATIONS OF MANET

Following are some of the applications of Mobile Ad Hoc Networks**:**

1.MANETs play a greater role in the Strategic networks such as automated battlefields. It is used for Communication purposes and for performing various operations in Military department.

2.During the time of any casualty the MANET offers support such as for search and rescue operations, for recovery of natural or manual disasters. It also supports the hospital staff such as doctors and nurses if any emergency related to patient arises.

3.MANETs have wider application in Electronic Commerce. The online booking of tickets, online shopping, online payment of bills etc. all are done by the help of MANETs. Vehicular Networks(VANETs) used for road safety are one of the best example of application of MANETs in civilian environment.

4.MANETs are also used at homes for Creating Personal Area Networks(PAN) in order to carry out the important work of the office or work from home purposes .Conferences, Meeting rooms, construction sites help people to communicate with each other by the using MANETs.

5. University and campus settings, Creation of Virtual classes for smart learning, Communication during meetings or lectures all are supported by MANETS. It helps a lot in saving the time and making efficient use of the technology for Education purposes:

6. Entertainment which is one of the basic demand of human beings for self creation and satisfaction are enhanced by the MANETs in the form of Multi user

games, Outdoor Internet access, Peer to peer Networking, Social networking etc.:

7.For communication and linking between Internet and Intranet, for extending cellular networks in an easy and efficient manner is done by the help of MANETs. Thus MANETs are used for Area Coverage extension:

4. PROPERTIES OF ADHOC ROUTING

The properties that are important in Ad-Hoc Routing protocols are:

(a)*Distributed operation*: The protocol should be distributed. It should not depend on a centralized controlling node .Wired networks also follow the same principle but the dissimilarity is that the nodes in an ad-hoc network can enter or leave the network very easily anytime.

(b)*Deadlock free*: To improve the overall performance, the routing protocol should assure that the routes present in the network are free from loops and do not form deadlocks. This helps in checking and avoiding the bandwidth and CPU consumption.

(c)*Demand based operation*: To minimize the network overhead and proper consumption of network resources the protocol should be reactive that is demand based. This means that the protocol should react only when needed and should not broadcast control information everytime.

(d)*Unidirectional link support*: Use of unidirectional links in addition to the bi-directional link improves the routing protocol performance.

(e)*Security*: The radio environment is exposed to outer attacks so to prepare the routing protocol to work properly some sort of security measures are to be followed. Authentication and Encryption is one of the ways to make the protocol more secured.

(f) *Power conservation*: The nodes in the ad-hoc network have limited power therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these special modes.

(g)*Multiple routes*: To reduce the number of problems due to topological changes and to avoid congestion, multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and therefore saving the routing protocol from initiating another route discovery procedure.

(h)*Quality of Service Support*: Some sort of Quality of service is necessary to include in the routing protocol. This helps to find for what kind of environment these Protocols can be used. Generally it could be for real time traffic support.

5. PROBLEMS IN ROUTING WITH MANET

(a)*Asymmetric links*: Most of the wired networks work with symmetric links that are always fixed. But symmetric links are not supported by Mobile ad-hoc networks because the nodes are mobile and constantly change their position within network.

(b)*Routing Overhead*: In wireless ad hoc networks, nodes generally change their location within network due to which some false routes are generated in the routing table which leads to undesirable routing overhead.

(c)*Interference*: In mobile ad-hoc networks links are made and broken depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can spoil the total transmission.

(d)*Dynamic Topology* :As the topology is not constant so the mobile node might move or network characteristics may get changed.

6. TYPES OF ROUTING PROTOCOLS IN MANET

Classification of routing protocols in mobile ad hoc network can be done depending on the type of strategy used for routing and the structure of the network .

1. According to the ***routing strategy*** routing protocols can be classified as Proactive(Table driven) and Reactive(Source Initiated).

2. According to the ***network structure*** routing protocols can be categorized as flat routing, hierarchical routing and geographic position assisted routing.

(a)*Flat Routing protocols***:** Flat routing protocols are divided into two classes: first class is proactive routing (table driven) protocols and other class is reactive (on-

demand) routing protocols. One thing is general for both protocol classes is that every node participating in routing play an equal role. They have further been classified on the basis of their design principles such as proactive routing is mostly based on LS (link-state) while reactive routing is based on DV (distance-vector).

*Proactive protocols:*These are traditionally shortest path protocols that are distributed in nature.These maintain the routes between every pair of node at all time.These work on the periodic updates criteria and have high routing overhead.

Reactive protocols: These are also known as demand based protocols. The route is determined at the time of need and the source initiates the discovery of the routes. There is no periodic update everytime

Hybrid protocols: These protocols have features of both the proactive and reactive protocols. It is used to find a balance between both protocols. Proactive operations cover small areas , whereas, reactive protocols are used for locating nodes outside those areas.

(b) *Hierarchical Routing protocols*: As the size of the wireless network increases, the flat routing protocols may lead to too much overhead for the MANET. In this case a hierarchical routing protocols are used.

(c) *Geographical Routing Protocols*: There are two approaches of geographic mobile ad hoc networks:

1. The actual geographic coordinates are obtained with the help of GPS – the Global Positioning system.
2. The reference points can be obtained in some fixed coordinate system anytime.

The geographic routing protocols save time to a greater extent in a network in order to search for the destinations. If the recent geographical coordinates are known then control and data packets can be sent in the general direction of the destination. This also reduces the control overhead in the network.

TABLE 1:Types of Routing Protocols in MANET

Mobile Ad hoc Routing protocols	
Flat Routing Protocols	**Proactive** 1.Optimized Link State Routing (OLSR) 2. Fish-eyeState Routing (FSR) 3. Destination-Sequenced Distance Vector (DSDV) 4. Cluster-head Gateway Switch Routing Protocol (CGSR)
	Reactive 1. Ad hoc On Demand Distance Vector (AODV) 2. Dynamic Source routing protocol (DSR) 3. Temporally ordered routing algorithm (TORA) 4. Associativity based routing (ABR) 5. Signal Stability-Based Adaptive Routing (SSA) 6. Location-Aided Routing Protocol (LAR)
	Hybrid 1.Zone Routing Protocol, (ZRP) 2. Wireless Ad hoc Routing Protocol, (WARP)
Hierarchal Routing Protocols	1. Hierarchical State Routing (HSR) 2.Zone Routing Protocol (ZRP) 3.Cluster-head Gateway Switch 4.Routing Protocol (CGSR) 5.Landmark Ad Hoc Routing Protocol (LANMAR)
Geographical Routing Protocols	1.GeoCast (Geographic Addressing and Routing) 2.DREAM(Distance Routing Effect Algorithm for Mobility) 3.GPSR (Greedy Perimeter Stateless Routing)

7. SECURITY PROBLEMS IN MANETS :

MANETs are much more exposed to attacks. The possible security attacks in MANETs can be divided into two classes

- Damaging Route Logic : When incorrect routing control messages get injected into the network and damage the routing logic.

- Traffic Deformation Attack: All attacks that do not allow some or all data packets to transfer from the source to the destination, belong to the category of Traffic Deformation Attack. This type of attack can lead to snooping of network traffic, corrupt the packet header or contents, block transmissions for some harmful purposes.

Some of the attacks in MANETs are:

(a)*Snooping*:Due to the broadcast nature of the radio signals there arrises the problem of overhearing the packets. The two types of information that is obtained by overhearing are:

(1)Packet Payload Data: The actual data present in the packet is obtained if proper encryption is not applied to the packet.
(2)Routing Information: The route between the source and the destination gets revealed by snooping as a result the privacy of the network gets harmed to a greater extent.

Cryptography is one of the best way to maintain the privacy of the network.

(b)*Jamming*: An interference can take place with radio waves because WLANs1 use unlicensed radio frequencies, other infrared waves may overlap with WLANs and harm the network .This condition is known as jamming.

There are two types of Jammers:

- High power pulsed full band jammers.
- Low power partial-band jammers.

Jamming can be reduced by using spread spectrum that is designed for resisting the interference and noise in the network. Receiver uses the same code as the transmitter therefore narrow down the signal to original form.

There are two types of Spread spectrums:

(1)Frequency Hopping Spread Spectrum(FHSS):In this the radio signals are sent over multiple channels. At a time only one channel is active. Hopping Sequence is determined by Pseudo random code sequence. Only receiver can narrow down the signal.

(2)Direct Sequence Spread Spectrum(DSSS):In this spectrum 11 bit chipping sequence is used and the data ic converted to waveforms. These waveforms are transmitted over a frequency range .Receiver unspreads the chip to recover the original data.

There is a problem that due to inherent characteristic of Jamming the above mentioned countermeasure does not completely removes the Jamming.

(c)*Packet Modification and Dropping*: The immediate nodes present in the network can modify the content of the packets if no proper integrity constraints are used. The header of the Source and destination addresses may even get changed. Any node can act as router. There can be any type of dropping such as Selective Dropping, Constant Dropping, Periodic Dropping and Random Dropping

The proper integrity constraints to be used to protect the content of the packet from being modified and dropped.

(d) *Flood Storm Attack*: It is kind of denial of service attack. Malicious nodes perform the flooding of packets by using false or meaningless PREQ and RREP messages. The main motive of this type of attack is to immobilize the network and cosume the bandwidth of the network.

Authentication of the control messages is one of the methods that can be adopted to reduce the effect of flood storm attacks.

(e) *Identity Impersonation*: The attacker can achieve various harmful goals by impersonating another user. The IP address and MAC based identity are easy to impersonate, if communication channel is not secured. The Authentication scheme if not used properly results into this type of attack.

(f)*Repeater Attack*: In this attack, a malicious node repeats or replays the packets of one of its neighbour . This result into misconception to the other side neighbour assuming that the node whose packet have been replayed is its neighbour, but in reality it is not. Now the malicious node can selectively replay packets between the two nodes, while dropping other packets. This would cause a Denial of Service for the nodes. This phenomenon is not very simple to examine because nodes can assume that this periodic dropping is because of the noisy channel.

One of the method for detecting these attacks is by making use of Secure Neighbour Detection Techniques.

*(g)Wormhole attack***:** It is the most general form of the repeater attack. This type of attack makes use of the tunnelling concept to transfer the data. The attacker saves the packet at one location sends it to second location with the help of tunnel. Then the attacker keeps on replaying the packets from the second location. The main requirement of such type of attacker is only two nodes in order to harm the transmission. The tunnel that is used for communication can be Wired or wireless. If the distance between the two end points of the tunnel is greater than the radio coverage of the two nodes than that tunnel is the warmhole attack which harms the security.

(h)*Black Hole Attack*: It is the most common attack in Mobile Ad Hoc Networks. The node which supports this type of attack is known as black hole node or malicious node. It is a node which transmits the false data in a network between the reliable nodes. A black hole responds to the Route Request(RREQ) messages sent by the sender to the destination. It sends Route Reply(RREP) messages in reply even if it does not have any valid route between source and destination .As a result of this the sender gets false information and thusthe packet gets dropped rather than being forwarded in the network. This situation becomes very harmful if black hole declares itself as the node having the shorter path to almost every node in the network. This results in the total dropping of packets and giving rise to the problem of denial of service.

8. CONCLUSION

In this paper we have discussed the Infrastructure less Mobile Ad hoc Network. In the first part we have given the brief description of Mobile Ad hoc network such as its history, types of MANET etc. In the second and third part the characteristics and applications have been discussed. In the fourth part the properties of routing protocols being used in Ad hoc networks have been discussed. In the fifth part the Routing Problems of the MANET is described. The sixth part includes the types of routing protocols. The last part introduced is the most important issue that is the security issue of the MANETs. We concluded that MANETs being an infrastructure less networks have security and privacy issues and there are many attacks which harm the integrity of the Mobile Ad hoc Networks. The MANETs are being used at large levels in todays' world so they need to get secured and protected for the proper working of the infrastructure less networks.

REFERENCES

[1] Krishna Paul,Dirk Westhoff"Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks",2002

[2] Sanjay K. Dhurandher,Mohammad S. Obaidat,Mukta Gupta "A Reactive Optimized Link State Routing Protocol for Mobile Ad hoc Networks",2010

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Session 4

[4] Abhishek Seth" Security Issues in MANETs"Seminar report,Novembe 12,2004

[5] Jagtar Singh, Natasha DhimanDepartment of Computer Science & Engineering HCTM Technical Campus, Kaithal, India "A Review Paper on Introduction to Mobile Ad Hoc Networks" under International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 2

[6]Robinpreet Kaur & Mritunjay Kumar Rai, Department of Electronics and Engineering, Lovely Professional University, Phagwara, Punjab,India "A Novel Review on Routing Protocols in MANETs" under Undergraduate Academic Research Journal (UARJ), ISSN : 2278 –1129, Volume-1, Issue-1, 2012\

[7] Ankur O. Bang 1, Prabhakar L. Ramteke2" MANET : History,Challenges And Applications" *International Journal of Application or Innovation in Engineering & Management(IJAIEM)* Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com Volume 2, Issue 9, September 2013

[8] Karan Singh, R. S. Yadav, Ranvijay "A REVIEW PAPER ON AD HOC NETWORK SECURITY" under International Journal of Computer Science and Security, Volume (1): Issue (1)

[9] Lu Han, October 8, 2004 "Wireless Ad-hoc Networks

