An Overview on MANET- Advantages, Characteristics and Security Attacks

Prabhleen Kaur
Research Scholar
BGIET
Sangrur, India

Sukhman
Assistant Professor
BGIET
Sangrur, India

ABSTRACT
Wireless technology has brought a very advance change in the field of internet. It has given rise to many new applications. In recent years, a lot of work has been done in the field of Mobile Ad hoc Networks (MANET) that makes it so popular in the area of research work. MANET is an infrastructure-less, dynamic network. It consists of collection of wireless mobile nodes, and the communication between these nodes has carried out without any centralized authority. In this paper the discussion has been carried on the characteristics, challenges, applications, security goals and different types of security attacks of MANET.

Keywords
MANET, Routing Protocols of MANET, Attacks in MANET.

1. INTRODUCTION
Mobile Ad-hoc Network is a self-organizing and self-configuring multi-hop wireless network where the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. The nodes in the network not only act as hosts but also as routers that send the data from one node to the other node in the network. [11] Each node in the MANET uses wireless interface to communicate with the other nodes. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure such as access points or base stations. [4]

Fig 1: Mobile Ad hoc Network (MANET) [5]

2. EVOLUTION OF MANET
All 2.1 In 1970, Normanl Abramson and his fellow researchers at the University of Hawaii invented ALOHAnet.

2.2 In 1972 DARPA Packet Radio Network (PRNet)

2.3 In 1980 Survivable Radio Networks (SURAN).

2.4 During 1980 emergence of Internet Emerging Task Force (IETF), termed the mobile ad hoc networking group.

2.5 In 1994 emergence of Bluetooth by Ericsson. [10]

3. CHARACTERISTICS OF MANET
Mobile Ad hoc Network is a collection of autonomous and mobile elements such as laptops, smart phones, wearable computers, tablet, PC, PDA etc. The mobile nodes can dynamically self-organize in arbitrary temporary network topology. Some main characteristics of MANET are discussed below: [2]

3.1 Infrastructure less
MANET is an infrastructure less network. It does not require any specialized hardware to make connection between nodes. All nodes communicate with each other through the wireless link. [2]

3.2 Multi hop routing
When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes. [4]

3.3 Autonomous terminal
In MANET, each mobile node is an independent node, which could function either as a host or as a router. [4]

3.4 Dynamic topology
Nodes are free to move arbitrarily in any direction with different speeds; thus, the network topology gets changed randomly at any time. The nodes in the MANET dynamically establish routing among them as they travel around and them establishing their own network. [4]

3.5 Light-weight terminals
In maximum cases, the nodes used in MANET are mobile with less CPU capability, low power storage and small memory size. [4]

3.6 Bandwidth-constrained and variable capacity links
Wireless links have significantly lower capacity then their hardwired counterparts. Due to multiple access, noise, and interference conditions, the capacity of a wireless link degrades over time and the effective throughput may be less than the radio's maximum transmission capacity. [2]

4. ADVANTAGES OF MANET
4.1 Router Free
Connection to the internet without any wireless router is the main advantage of using a mobile ad hoc network. Because of this, running an ad hoc network can be more affordable than traditional network. [2]

4.2 Fault Tolerance
MANET supports connection failures, because routing and transmission protocols are designed to manage these situations. [2]

4.3 Cost
MANET could be more economical in some cases as they eliminate fixed infrastructure costs and reduce power consumptions at mobile nodes. [2]

5. DISADVANTAGES OF MANET

5.1 Bandwidth Constraints
The bandwidth of the wireless links is always much lower than in wired counterparts. Indeed, several Gbps are available for wired LAN, while, nowadays, the commercial applications for wireless LANs work typically around 2 Mbps. [2]

5.2 Energy constraints
The power of the batteries is limited in all the devices, which does not allow infinitive operation time for the nodes. Therefore, energy should not be wasted and that is why some energy conserving algorithms has been implemented. [2]

5.3 High Latency
In an energy conserving design nodes are sleeping or idle when they do not have to transmit any data. When the data exchange between two nodes goes through nodes that are sleeping, the delay may be higher if the routing algorithm decides that these nodes have to wake up. [2]

5.4 Transmission Errors
Attenuation and interferences are other effects of the wireless link that increase the error rate. [2]

6. APPLICATIONS OF MANET

6.1 Tactical networks
Military Communication automated Battle fields

6.2 Sensor Network
Remote weathers for sensors, earth activities

6.3 Emergency Services
Disaster recovery, earthquakes, crowd control and commando operations

6.4 Educational Applications
Setup virtual class & conference rooms

6.5 Entertainment
Multi-user games, robotics pets.

6.6 Location Aware Services
Automatic Call forwarding, advertise location specific services, Location–dependent travel guide. [10]

7. ROUTING PROTOCOLS OF MANETS
Main function of routing protocol is to find the path between the sender and the receiver. If nodes are in direct range of each other then they can directly connect and can communicate with each other , but if in case nodes are not in direct range then they need some intermediate nodes to transfer their data packet Basically in MANET there are three types of routing protocols i.e. Proactive, Reactive and hybrid.

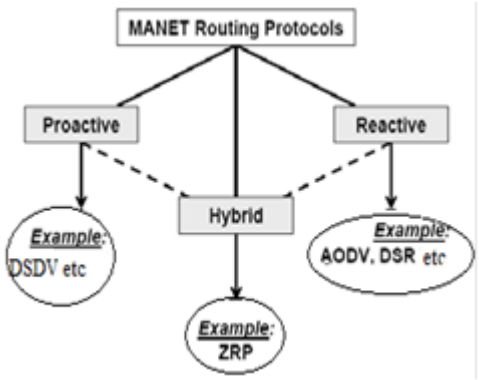

Fig 2: Classification of Routing Protocols [4]

7.1 Proactive Routing Protocols
Proactive routing protocols are also called as table driven routing protocols. In this every node maintain routing table which contains the full information of all the nodes present in the network. The routing tables are updated periodically after a small time interval. Proactive protocols are not suitable for large networks as they need to maintain full information of all the nodes present in the network. This causes more overhead in the routing table leading to consumption of more bandwidth. Example: DSDV. [1]

7.1.1 Destination Sequenced Distance Vector
(DSDV) - DSDV is developed on the basis of Bellman–Ford routing algorithm with some modifications. In this routing protocol each node maintains a routing table that contains the full information of all the other nodes present in the network. Each table entry is tagged with a sequence number, which is originated by the destination node. Periodic transmissions of updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. DSDV protocol requires each mobile node in the network to advertise its own routing table to its current neighbors. The advertisement is done either by broadcasting or by multicasting. [1]

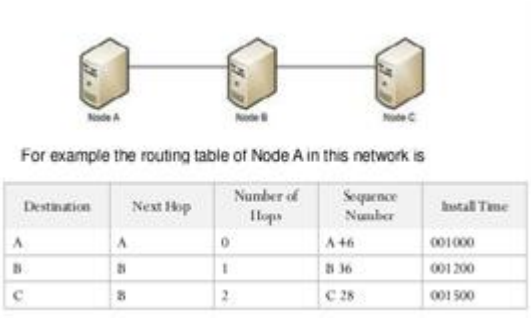

Fig 3: Destination Sequenced Distance Vector (DSDV)

7.2 Reactive Routing Protocol
Reactive routing protocols are also known as on-demand routing protocols. These protocols do not maintain the routing information of all the nodes present in the network at all the time. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection between sender and receiver so that they can communicate with each other. Reactive routing protocols are more popular because they require less bandwidth and there is no extra wastage of memory. Example DSR.

7.2.1 Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a reactive protocol based on the source route approach. In Dynamic Source Routing (DSR), the protocol is based on the link state algorithm in which source initiates route discovery in an on demand manner The sender determines the route from source to destination and it includes the address of all the intermediate nodes in its routing table.. DSR was designed for multi hop networks with small diameters. It is a beaconless protocol in which no HELLO message is exchanged between the nodes. [1]

7.3 Hybrid Routing Protocol

Hybrid routing protocols combination of both reactive and proactive routing protocols. [7] Proactive protocols have large overhead and less latency while reactive protocols have less overhead and more latency. So a Hybrid protocol is invented to overcome the shortcomings of both proactive and reactive routing protocols. Hybrid protocol is suitable for large networks. In this, large network is divided into set of zones where routing inside the zone is performed by using reactive approach and outside the zone routing is done using reactive approach. Example: ZRP. [1]

7.3.1 Zone Routing Protocol

The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extra memory. [4] ZRP is suitable for wide variety of MANETs, especially for the networks with large span and diverse mobility patterns. In this protocol, each node proactively maintains routes within a local region, which is termed as routing zone. Route creation is done using a query-reply mechanism. For creating different zones in the network, a node first has to know its neighbors. A neighbor is defined as a node with whom direct communication can be established and that is within one hop transmission range of a node. [1]

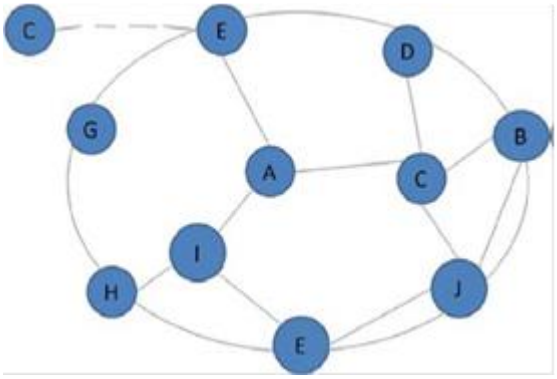

Fig 4: Neighbor's of ZRP [7]

Components of ZRP are:

7.3.1.1 Intra-zone Routing Protocol (IARP)

IARP is used to communicate with the nodes which are present within the zone.

7.3.1.2 Inter-zone Routing Protocol (IERP)

IERP is global reactive component of ZRP. It is used to communicate with nodes which are present outside of the zone.

7.3.1.3 Boardercast Resolution Protocol (BRP)

BRP is used to direct the route request initiated by global reactive IERP. It is used to maximize efficiency and increase disused queries. [7]

Table 1. Comparison of Routing Protocols [5]

Paramètres	**Proactive Protocol**	**Réactive Protocol**	**Hybrid Protocol**
Routing Structure	Flat and Hierarchical	Flat	Hierarchical
Availability of Routes	Always available	Created when needed	Depend on the destination location
Scalability	100 nodes	>100	>1000
Route Mobility	Low	High	Very High
Delay	Small (routes are already known)	High (routes are discovered on demand)	For local destination small, for inter-zone it may be large as reactive protocol.
Information of Routing	Information stored in routing tables	Is not stored	According to need if required

8. ATTACKS IN MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. There are number of attacks that affect MANET. The two basic attacks are: [9]

8.1 Passive attack

A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. [4]

8.2 Active attack

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are present within the network, internal attacks are more severe and hard to detect than external attacks. [4]

8.1.1 Blackhole Attack

In this type of attacks, malicious node claims having an optimum route to the destination node whenever it receives RREQ packets, and sends the REPP with highest destination sequence number and minimum hop count value to originator node. For example, in figure 5, when node "S" wants to send

data to destination node "D", it initiates the route discovery process. The malicious node "M" when receives the route request, it immediately sends response to source. If reply from node "M" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node "M". As a result, all data packets are consumed or lost at malicious node. [4]

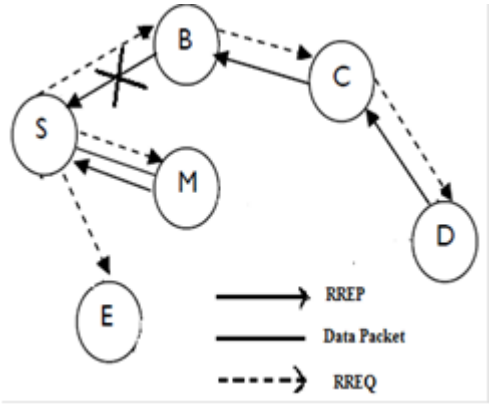

Fig 5: Blackhole Attack [4]

8.1.2 Wormhole Attack

In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. For example in figure 6, the nodes "X" and "Y" are malicious node that forms the tunnel in network. The Originating node "S" when initiate the RREQ message to find the route to node "D" destination node. The immediate neighbor node of originating node "S", namely "A" and "C" forwards the RREQ message to their respective neighbors "H" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbor node "B", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-A-B-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus, invalidates the legitimate route <S-C-H-E-F-D>. [4]

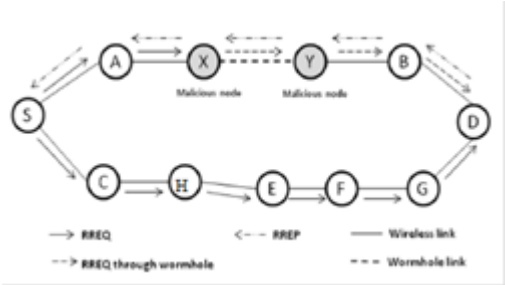

Fig 6: Wormhole Attack [4]

8.1.3 Gray-hole attack

This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability. [9]

9. CONCLUSION

In this paper, we give a brief introduction about MANET in which we come to know that where MANET can be used in our environment which provides safety from disasters. Also we study about the attacks which can affect our network.

10. REFERENCES

[1] Dhenakaran S.S (Dr.), ICARCSSE, "An Overview of Routing Protocols in Mobile Ad-Hoc Network", Vol.3, Issue: 2, ISSN: 2277-128X, pp: 251-259 (2013).

[2] Bakshi Aditya et.al, IJITEE, "Significance of Mobile Ad-Hoc Network (MANET)", Vol.2, Issue: 4, ISSN: 2278-3075 (2013).

[3] Sekhar Chandra P. et.al, IJCTA, "A Survey on MANET Securing Challenges and Routing Protocols", Vol.4 (2), ISSN: 2229-6093, pp: 248-256 (2013).

[4] Aarti, IJARCSSE, "Study of MANET: Characteristic, Challenges, Applications and Security Attacks", Vol.3, Issue: 5, ISSN: 2277-128X, pp: 252-257 (2013).

[5] Bansal Ekta, "Improving Performance of AODV Using ANT Agents" (2013).

[6] Bang O.Ankur et.al, IJAIEM, "MANET: History, Challenges and Applications", Vol.2, Issue 9, ISSN: 2319-4847, pp: 249-251 (2013).

[7] Kaur Harjeet et.al, IJCSIT, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", Vol.4 (3), ISSN: 0975-9646, pp: 498-500 (2013).

[8] Kumar Mohit et.al, IJCSE, "An Overview of MANET: History, Challenges and Application", Vol.3 No. 1, ISSN: 0976-5166, pp: 121-125 (2012).

[9] Goyal Priyanka et.al, IJCEM, "MANET: Vulnerabilities, Challenges, Attacks and Applications", Vol.11, ISSN: 2230-7893, pp: 32-37 (2011).

[10] Ghosekar Pravin et.al, IJCA, "Mobile Ad-Hoc Networking: Imperatives and Challenges", pp: 153-158 (2010).

[11] Gorantala Krishna, "Routing Protocols in Mobile Ad-Hoc Network" (2006).