Mobile Ad-Hoc Networking (MANET)

Muhammad Zunnurain Hussainf[a], *Muhammad Zulkifl Hasan* [b] ✉ *and Zaka Ullah*[c]

[a] zunnurain.bulc@bahria.edu.pk,

Assistant Professor, Bahria University Lahore Campus ,Senior Lecturer LGU Lahore, Pakistan

✉, [b] zulkifl@ncbae.edu.pkzakaullah@lgu.edu.pk
Assistant Professor, NCBAE Lahore, Pakistan

ABSTRACT

Mobile Ad Hoc Networks (MANETs) is a class of wireless networks that do not need any infrastructural support. MANETs can adapt and reconfigure its structure while running in response to the changing network topologies. This makes MANETs attractive to the military because of its random nature which could be beneficial in the tactical environment like in the military. MANET application, characteristics, limitations, its different types, and security concerns are discussed in this article.

Keywords: *MANET, topology, infrastructure, application, characteristics, limitations.*

1. INTRODUCTION

A Mobile Ad Hoc Network is a system of wireless node which are interconnected and communicate with each other over links constrained by bandwidth [1]. These wireless nodes perform as receiver, sender, or even a router. When the node acts as a sender, messages can be transmitted to any nodes within the network. When acting as a receiver, a node can receive messages from any other nodes. When it is a router, a node can send the packet to its destination or to the next router. Each node can buffer the packet waiting for transmission if it is necessary [1][2].

The movement of nodes is random, which is why an ad-hoc network works between the participating nodes, causing random changes in the network. As MANETs are a class of wireless networks, wireless users can form the network dynamically and do not need any infrastructural setups [1][2].

A Wired organization involves base stations, passages, and doors. Distant frameworks are associated through fixed switches, center points, and switches, though, in an impromptu organization the area of switches, centers, and switches might be portable. At a state of time, the quantity of switches can develop or decrease. Likewise, the courses may fluctuate in an impromptu organization. A versatile impromptu organization (MANET) is a structure remote specially appointed organization that incorporates an assortment of remote gadgets known as portable hubs once in a while called mobiles associated by remote connections [18]

MANETs are intended to work without fixed foundation and give solid interchanges to ground vehicles, boats, airplane, or people and structure a self-recuperating network that will empower persistent correspondences in any event, when at least one of its hubs are incapacitated or incidentally eliminated from the organization. Nonetheless, MANETs have demonstrated more hard to create for huge organizations with hundreds or thousands of hubs than was initially envisioned. Early MANET plans expected they could be scaled to extremely huge topologically level organizations where each hub in the organization has the equivalent ability and admittance to the remote channel. [17]

MANET is the quickly developing innovation that permits clients to impart with no actual foundation paying little mind to their area, which is the reason it is additionally alluded to as an "framework less" network [3].

The most well-known hubs of MANETs are cellphones, PCs, palmtops or any gadget remote gadget which are lightweight and works on a battery [4].

The routing protocols help in building up a correspondence way among source and objective. The steering conventions fall into three classes: proactive, responsive, and mixture. Proactive directing conventions are likewise named as table-driven steering conventions. These conventions keep up directing data as tables at each hub and the tables are refreshed at whatever point there is an adjustment in the geography of the organization. Receptive directing conventions are additionally named as on-request steering conventions. Receptive steering conventions don't keep up the geography data of the organization. They acquire the way and directing data is traded, just when the source hub and the objective hub need to speak with one another.[19]

2. CHARACTERISTICS OF MANET

There are a number of characteristics for MANETs, some of which are explained below:

A.Dynamic Network Topologies

MANET nodes move individually in any direction freely. The topology of the network may see changes persistently at unpredictable times consisting of only bidirectional links [5][6].

B.Low Bandwidth

MANETs range of transmission is shorter than networks with fixed infrastructure. Wireless communication network’s throughput is less than wired communication due to the effect of multiple access, fading, noise, and interference conditions [5].

C. Limited Battery Power

For MANETs energy conversation is most important because nodes rely on smaller batteries and different forms of energy which do not last for too long [5][6].

D. Unreliable Communications

Wireless links have unstable channel quality and being shared-medium in nature which could result in high packet-loss rate and rerouting instability, which is common in multi-

hop networks and could lead to throughput drop. This implies that in wireless ad hoc networks security cannot rely on reliable communications [7].

E.Scalability

In mobile devices processing speed and memory is limited and when large networks are concerned, scalability is a major issue. Even when networks of 10,000 or 100,000 are envisioned, scalability remains a major concern for wireless communication networks [6].

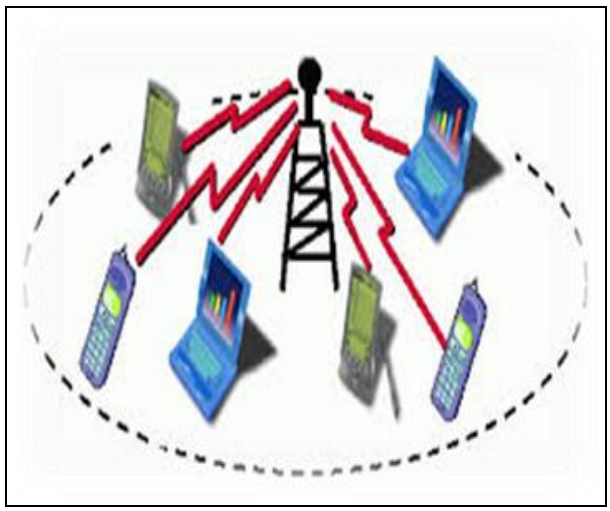

Figure 1 Infrastructure based wireless network

F.Weak Physical Protection

MANETs are weaker towards security threats than wired networks due to the mobile node being compact, soft and hand-held in nature. Since mobile devices are getting smaller and smaller the chances of damaging or getting lost are increasing [5].

G. Decentralized Control

Since links in MANET are unreliable, it depends on how well participating nodes cooperate with each other. It means that implementing any protocol that uses administration right becomes a difficult task [6].

In addition to the above-mentioned characteristics, MANETs has limited physical security. MANETs are weaker to security threats like eavesdropping, interception and routing attacks than wired networks. So security cannot be compromised for these networks. Nodes in MANETs do not consume much energy and only transmit when it is necessary, decreasing the chances of any threats towards the security. In addition, the decentralized nature of these networks makes them more robust when chances of failure arise when compared to centralized networks [6].

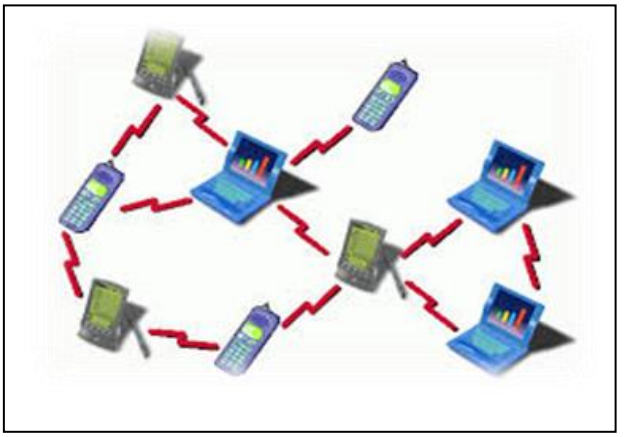

Figure 2 Ad-hoc wireless network [8]

.

3. METHODOLOGY

There are different methodologies to design and classify routing protocols for MANET. For example, exchanging of routing information, when and how it exchanges and how these routes are computed? Some classification of MANET protocols is listed below:

Pro-active (Table Driven) Routing

This routing protocol maintains a list of destinations and routes by distributing routing tables all over the network. There are some disadvantages of using this protocol the main one is that these protocols require data maintenance and are slow when reacting on restructuring. The most common protocols under this are:

- Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)
- Wireless Routing Protocol (WRP)
- Fisheye State Routing

Reactive (On-Demand) Routing

In these protocols, routes are found on demand which is done by flooding the consecutive requests of packets. The disadvantage of these algorithms is that high latency time in finding routes and too much flooding of the network can lead to a clog in the network. It is also called on-demand routing. The main Protocols are:

- Dynamic Source Routing Protocol (DSRP)
- Ad-Hoc On-Demand Distance Vector Routing Protocols (AODV)
- Temporally Ordered Routing Algorithm (TORA)

4. APPLICATION OF MANETS

MANET application are various and diverse some of which are as follows:

A. Military Tactical Operations

On a battlefield, the line of sight is thin between users who need to communicate in a dense environment. To provide on-field troops fast and short term sources of communications when the soldiers are deployed in a hostile environment to carry out missions [5][9].

B. Search and Rescue Operations

When soldiers are scouting an area with little to no wireless infrastructure support, thus rendering device depending on these networks useless, MANETs proves useful for communication between troops [5].

C. Disaster Relief Operations

In an environment where the existing infrastructure is either destroyed or is not operating due to some problems, MANETs are used because they do not need an infrastructural setup to make communication possible.

D. Law Enforcement

Security officers who are on patrol in an area with no infrastructural support can use MANETs for fast and secure communication [9].

E. Uses for Commercial Programs

MANETs can be used for communication in areas where a large number of people are gathered for some event like an exhibition, conference, or festival. It can also be used for business purposes, the collaboration between staff is more important when not working inside an office because there might be circumstances where staff members need to hold a meeting to discuss a project [5].

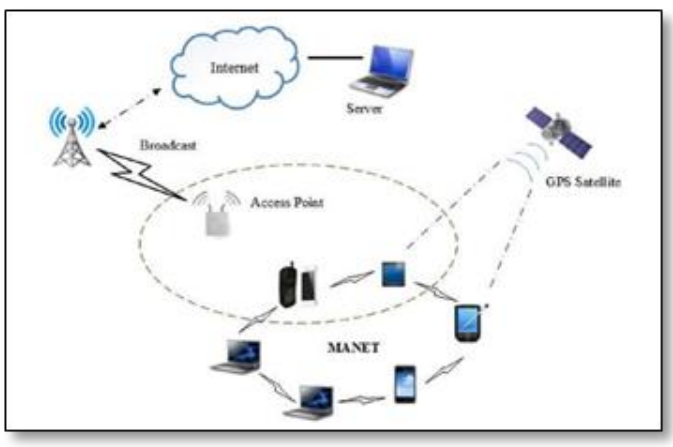

Figure 3 Applications of network [16]

5. TYPES OF MANET

MANETs have further been divided into three different types:

A. Vehicular Ad-hoc wireless network (VANET)

VANET, short for Vehicular Ad-hoc Network, is one of the subclasses of MANETs. It is a special class of wireless ad-hoc network with high mobility nodes and topology with a faster rate of change. VANETs uses moving vehicles as nodes and create a network around them. Every car within the VANETs range becomes a node, which in turn allows them to connect with each other and create a network [10].

Although vehicles within a specific range can create a connection with each other. As cars drop out of the network, due to increasing distance, other cars can join in connecting them to each other and making a mobile wireless network. These networks do not have infrastructural support and rely solely on the vehicles to create a network and provide a network's functionalities [12].

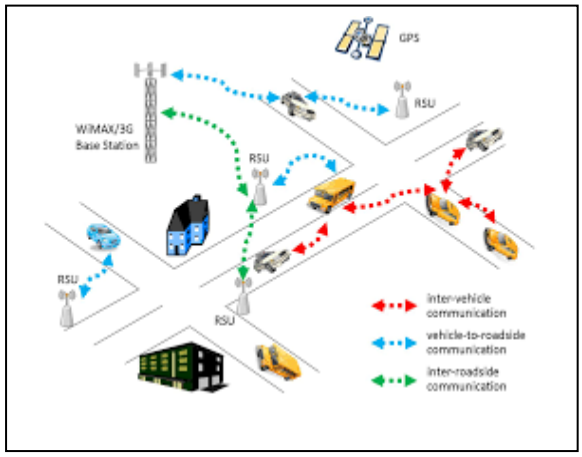

Figure 4 Vehicular Ad-Hoc wireless network [11]

B. Internet-Based Mobile Ad-hoc Network (IMANET)

MANETs linking mobile nodes with Internet-gateway nodes are known as Internet-Based Mobile Ad-hoc Networks (IMANET). With this type of network, normal routing algorithms do not apply directly. As MANETS do not need any infrastructural support to operate, these type of networks work best where no fixed infrastructure exists [12].

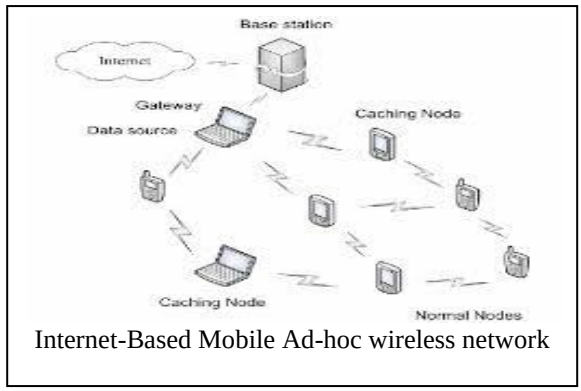

Figure 5 Internet-Based Mobile Ad-hoc wireless network [13]

C. Intelligent Vehicular Ad-hoc Network (InVANET)

Artificial intelligence designed to prevent any kind of accidents of vehicles for various reasons such as drunken driving, collisions, etc. is known as Intelligent Vehicular Ad-hoc Network (InVANET). Many ad-hoc networking technologies integrate VANET for convenient, precise, and effective communication between vehicles. InVANET helps in defining safety measures in vehicles and also for better communication between vehicles [12].

6. SECURITY GOALS

Since MANETs services are configured when it is in progress security is an important factor for MANET. If the security architecture is not properly designed from the start, when the time for deployment of the network comes it is can be hard to achieve the security goals designed for the network [6].

MANET security services are funded through a set of investments made by certain organizations interested in MANETs features. Since nodes perform all the network's functionalities themselves, securing a MANET is a difficult task and must be approached carefully [6]. To check if MANET is secure or not certain goals are used which are as follow:

A.Availability

When an authorized third party requires assets at an appropriate time and the assets are accessible it shows the availability of a program or a system. It is true for both data and services [6].

B.Confidentiality

Confidentiality of a system means that all of the assets which are related or dependent on a computer can only be authorized parties, which means no one other than authorized people can access the system. People with no privilege to access the system's information

should be kept away from the secret of confidential information. Confidentiality can also be referred to as privacy or secrecy [6] [14].

C. Integrity

The privilege of modifying a system should only be given to authorized parties since modification means changing a system's structure in either a good or bad way for the system, it should be limited to only trustful peoples. The integrity of a system makes sure that messages being sent can never be ruined [6].

D. Authentication

A node needs to make sure the identity of the neighboring node it is either in communication or going to communicate, this is referred to as authentication. Assuring that nodes communicating are authorized and not fake [6]. Since only an authorized node, whose identity is ensured, can produce, and send a message. The authenticity of a node is assured when a message is not being sent properly [15].

E.Anonymity

Information regarding the use of a node needs to be kept private and must not be distributed by the system or by the node itself, this procedure is known as anonymity [6]. This is done in order to prevent any unauthorized access to the node's information.

7. LIMITATIONS OF MANET

Despite all its applications and useful characteristics, MANETs still have various limitations that are yet to be taken care of [1].

A.Throughput Drops with More Hops

A node can transmit a packet to its neighboring node directly, but this does not hold for non-neighboring nodes. The packets are transmitted in between nodes, acting as routers, through a sequence of multiple hops, thus increasing the hop count which ultimately decreases throughput [1].

B.Throughput Drops with Increasing Mobility

Due to the unpredictable nature of MANETs, nodes that are highly mobile which results in more overhead. It is due to the increase of packet transmission because new routes need to be determined after route failures. When using a routing table, each node keeps a list of every available destinations and also the hops required to reach those destinations. Any change in the topology would affect the routing table, and when changes occur in a routing table it is passed on to every node, resulting in huge overhead on the network [1].

C. Delay

The average time a packet takes to reach its destination from its source is referred to as delay. Nodes need to be kept busy with repeated transmission and receiving of packets, so the throughput of the network could increase. This means the row of each node would remain void, leading to long delays [1].

8. FUTURE WORK

There is much work to be done on MANET to make it a technology that is perfectly reliable for the user and the engineers working behind the scenes. The future work which could possibly improve the technology are as follow:

- Transport Layer
- Routing Layer
- MAC Layer
- Architecture

Work on these features is being done and possible benefit MANET technology for good.

9. CONCLUSION

In this paper, we have discussed MANET characteristics, types, applications, limitations, and security goals. MANET is technology in networking that does not require support of infrastructure and can configure itself on-the-fly. As discussed in this article, different types of MANETs exist and operate in a different environment to provide communication between participating nodes. MANETs have to be secured due to their random nature which can be done by adhering to some security goals. While it is used in many fields as stated due to its nature many limitations are plaguing the networks which make it somewhat unstable. Many areas in this technology are yet to be refined and are currently being worked on for more benefits in the near future.

REFFERENCES

[1] C. Yuen, R. Seah, S. Soon, and T. Jia, "Mobile Ad Hoc Networking," *Dsta.gov.sg*. 2019.

[2] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Networks," *Infoscience*. 2019.

[3] Jonathan Loo, *Mobile Ad Hoc Networks Current Status and Future Trends*. Boca Raton: CRC Press, 2012.

[4] "Infrastructure based wireless network." 2019.

[5] S. Kumar and S. Kumar, "Study of MANET: Characteristics, Challenges, Application, Routing Protocol and Security Attacks," *Int. J. R D Eng. Sci. Manag. (ISSN 2393-865X)*, vol. 2, pp. 266–274, 2015.

[6] P. Goyal, S. Batra, and A. Singh, "A literature review of security attack in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 9, no. 12, pp. 11–15, 2010.

[7] W. Peng and X.-C. Lu, "On the reduction of broadcast redundancy in mobile ad hoc networks," *Dl.acm.org*. 2019.

[8] A. wireless Network, "Ad-hoc wireless network," *Ad-Hoc and mesh networks*, 2019. [Online]. Available: https://www.researchgate.net/figure/Infrastructure-Based-Wireless-Network-Delay-Tolerant-Networks-also-known-as-DTNs-are-an_fig3_290271816.

[9] P. Goyal, V. Parmar, and R. Rishi, "Manet: vulnerabilities, challenges, attacks,

application," *IJCEM Int. J. Comput. Eng. Manag.*, vol. 11, no. 2011, pp. 32–37, 2011.

[10] J.-Z. Sun, "Mobile ad hoc networking: an essential technology for pervasive computing - IEEE Conference Publication," *Ieeexplore.ieee.org*. 2019.

[11] "Vehicular Ad-Hoc wireless network," *Ad-Hoc and mesh networks*. 2019.

[12] K. Mahajan and H. Singh, "MANET its types challenges goals and approaches: A review," *Int. J. Sci. Res.*, vol. 5, no. 5, 2016.

[13] "Internet-Based Mobile Ad-hoc wireless network," *Ad-Hoc and mesh networks*, 2019. [Online]. Available: https://www.researchgate.net/figure/Infrastructure-Based-Wireless-Network-Delay-Tolerant-Networks-also-known-as-DTNs-are-an_fig3_290271816.

[14] S. Gupte and M. Singhal, "Secure routing in mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 151–174, 2003.

[15] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks," 2003.

[16] S. K. S. S Suresh Kumar, Overview (Advantages and Routing Protocols).

[17] E. S. a. D. Gonzales, Optimal Number of Gateways for Mobile Ad-Hoc Networks.

[18] S. M. K. M. K. Muralidhar, An investigation into the operational limitations of mobile ad hoc networks, 2017.

[19] S. L. M. a. P. D. Dorge, Design and Performance Analysis of Mobile Ad, INDIA, 08 February 2018.