e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.529

Volume 9, Issue 7, July 2021

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

An Overview on Manet- Application, Merits, Demerits, Challenges, Characteristics and Security Attacks

Ashutosh Vashist
Research Scholar, PH.D (Computer Science),
Department of Computer Science.
School of Engg. & Tech.
Om sterling global University
Hisar (Haryana), India.

***Abstract:** The mobile ad hoc network is the type of network in which mobile nodes can join or leave the network when they want. Due to self-configuring nature of the network malicious nodes enter which are responsible to trigger various types of active and passive attacks.*

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. Mobile Ad hoc Network is an ad hoc network that can be formed to allow nodes to communicate without any infrastructure. The setup of MANET makes it very popular as compared to the traditional wireless network. In traditional wireless network, mid-point is required for overall process of the network, whereas MANET is self-organized and infrastructure-free network, which is considered as a good approach for some specific applications such as battlefield survivability, communication in the natural or manmade disaster areas, emergency or rescue operations.

In this paper the discussion has been carried on the characteristics, challenges, applications, security goals and different types of security attacks of MANET.

***Keywords:** MANETS, Attacks in MANET, Application, security attacks, Ad hoc Networking.*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an infrastructure less‖ network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network.[i] Ad hoc networks allow the device to maintain its connection and facilitate to remove or add devices from the network. The topology of ADHOC networks is also not stable it changes rapidly and randomly over time. There is no central authorization or centralized infrastructure to maintain the connections. Due to the absence of centralized authorization and vary topology the message routing is a big problem but the nodes themselves execute the message delivery. In the static networks, the packet is the route from source to destination, which is based on the shortest path and given the cost of function to extend this method in MANET, is difficult. In military operation and disaster recovery scenarios, Mobile Ad-hoc Network (MANET) has emerged as a key enabler in facilitating effective operation. The important traits that resulted in the widening popularity of MANET are quick to deploy ability and reconfigurability on the fly. In a disaster scenario, where probably the pre-existing communication infrastructures might have been destroyed, MANET can come into play in providing Internet connectivity. As nodes in a MANET move around, a routing algorithm for packet exchange between a pair of nodes plays significantly an important role in throughput and end-to-end delay performance. Several factors can affect the behaviour of routing protocols, including nodes mobility.[ii]

II. Mobile Ad Hoc Network

III. Application of MANET

With the increase of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications. Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infra structured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include [iiiiv]

Military Battlefield: Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

Local Level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

Personal Area Network (PAN): Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.

MANET-VoVoN: A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels.[v] Following are the major application areas of MANET

- Emergency Services
- Disaster Management
- Tactical Networks
- Education
- Entertainment
- Home & Enterprise Networking
- Convergence Extension
- Military
- Sensor Networks
- Context aware services

IV. Merits of MANET

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. Fault Tolerance

MANET supports connection failures, because routing and transmission protocols are designed to manage these situations.

3. Cost

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

V. Demerits of MANET

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. 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.

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.[vi]

VI. Security Challenges in Manet

MANETs comprise of the most exciting networks. MANETs are exposed to a variety of active as well as passive attacks since it makes use of air and hostile environments as a medium. Active attacks are conducted by opponents that are fully equipped with high-tech tools. They can modify data transmitted through the network as well as corrupting the functionality of the system by making alterations in link-related updates, topology and routing. Examples of active attacks include Blackhole attack, impersonation, DoS, Byzantine attack, Distributed DoS, wormhole attack, etc. On the other hand, passive attacks are performed by opponents that have insufficient abilities. Passive attacks are exemplified by traffic analysis, eavesdropping, etc. Some open issues and fundamental limitations of MANET security aspects have been discussed in this section.

A. Distributed Management

No centralized management can be established in MANETs owing to its ad hoc installation and peer-to-peer characteristic of nodes. Due to the absence of this centralized control and distributed nature of the network, maintenance of new node generations, loss of control in topology changes, authenticating new nodes and secure data distribution as well as keying information are affected. Furthermore, it also makes attack detection complex since no central point monitors the traffic in such a large-scale and very dynamic ad hoc network.[vii]

B. Limited Resource

There is a shortage of bandwidth, power resources, and computational constraints in ad hoc networks due to temporal and ad hoc deployment in harsh environments with limited resources. Ad hoc networks have become a playground for both developers and attackers owing to the restricted resources, and its solution space has also been significantly affected.[viii]

C. Cooperativeness

MANETs have transformed from client-server networks to cooperative networks owing to the absence of a central manager and peer-to-peer architecture. This collaborative nature seeks trust among the network nodes during routing or any data exchange. A change in this cooperative nature results in compromised or selfish nodes establishing necessitates forced cooperation among MANET nodes and customized MANET security solutions[ix], [x].

D. Dynamic Topology

Energy depletion in nodes, node mobility, physical hurdles, and node revocation due to actions against selfish and malicious nodes and node compromises, due to the dynamic nature of MANET necessitates adaptive security solutions.

E. Wireless Medium

The free access provided to the wireless medium in MANETs makes it vulnerable to various attacks like active interference and eavesdropping. Malicious nodes can make use of this wireless medium for injecting spoofed packets or modifying other mobile node transmissions.

F. Infrastructure-less

No specific infrastructure is available in MANETs to address security services like certificates, key distribution, etc.

G. Threats from Compromised Nodes within the Network

The risks from the nodes compromised within the network can be more threatening when attackers possess the valid decryption as well as encryption keys and utilise them to perform malicious actions. Also, such attackers attempt to conduct new attacks not known to the secure system[xi].

H. Absence of Secure Boundaries

MANETs fail to provide safe boundaries from the outside surroundings for securing against undesirable access to the network, thereby making it vulnerable to passive attacks.

VII. 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

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.[xii]

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.

3 Autonomous terminal

In MANET, each mobile node is an independent node, which could function either as a host or as a router.

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.

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.[xiii]

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.[xiv]

VIII. Attacks in MANET

These attacks can be classified into two types:

1. **External Attack**: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

2. **Internal Attack**: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

3. **Denial of Service attack**: 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. The attacker generally uses radio signal jamming and the battery exhaustion method.

4. **Impersonation**: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

5. **Eavesdropping:** This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

6. **Routing Attacks:** The malicious node make routing services a target because it's an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

7. **Black hole Attack:**: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[xv] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

8. **Wormhole Attack:** In a wormhole attack, an attacker receives packets at one point in the network, ―tunnels‖ them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

9. **Replay Attack:** An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

10. **Jamming:** In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

11. **Man- in- the- middle attack:** An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender. **10 Gray-hole attack**: This attack is also known as routing misbehaviour 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.

IX. 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.

References

[i] Priyanka Goyal1, Vinti Parmar2, Rahul Rishi3 MANET: Vulnerabilities, Challenges, Attacks, Application IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

[ii] P. Chitra1, T. Ranganayaki2, A Study on Manet: Applications, Challenges and Issues International Journal of Engineering Research & Technology (IJERT) ICATCT – 2020

[iii] M. Frodigh, P. Johansson, and P. Larsson.―Wireless ad hoc networking: the art of networking without a network,‖ Ericsson Review,No.4, 2000, pp. 248-263.

[iv] HaoYang, Haiyun & Fan Ye ― Security in mobile ad-hoc networks : Challenges and solutions,‖, Pg. 38-47, Vol 11, issue 1, Feb 2004.

[v] Luis Bernardo, Rodolfo Oliveira, Sérgio Gaspar, David Paulino and Paulo Pinto A Telephony Application for Manets: Voice over a MANET-Extended JXTA Virtual Overlay Network

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

[vii] S. Kumar, and K. Dutta, "Securing Mobile Ad Hoc Networks: Challenges and Solutions", International Journal of Handheld Computing Research, vol. 7, no. 1, pp. 26-76, 2016.

[viii] A. Kumar, V.K. Katiyar, and K. Kumar, "Secure Routing Proposals in MANETs: A Review", International Journal in Foundations of Computer Science & Technology (IJFCST), vol. 6, no.1, pp. 21-35, 2016.

[ix] K.R.K. Reddy, "Consequence of Security Attacks in MANET", International Journal of Scientific Research in Science and Technology, vol. 3, no. 8, pp. 1346-1352, 2017.

[x] B. U. I. Khan, R. F. Olanrewaju, M. M. U. I. Mattoo, A. A. Aziz, and S. A. Lone, "Modeling Malicious Multi-Attacker Node Collusion in MANETs via Game Theory", Middle-East Journal of Scientific Research, vol. 25, no. 3, pp. 568-579, 2017.

[xi] S. Kumar, and K. Dutta, "Securing Mobile Ad Hoc Networks: Challenges and Solutions", International Journal of Handheld Computing Research, vol. 7, no. 1, pp. 26-76, 2016.

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

[xiii] S. Sarika, A. Pravin, A. Vijayakumar, and K. Selvamani, "Security Issues In Mobile Ad Hoc Networks", in 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), 2016, pp. 329-335.

[xiv] S. Kumar, and K. Dutta, "Securing Mobile Ad Hoc Networks: Challenges and Solutions", International Journal of Handheld Computing Research, vol. 7, no. 1, pp. 26-76, 2016.

[xv] Broch,J., A.M David and B. David,1998. A Performance comparison of multi-hop wireless ad hoc network routing protocols. Proc.IEEE/ACM MOBICOM'98, pp: 85-97.