Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Mobile Ad-hoc Network: Characteristics, Applications, Security Issues, Challenges and Attacks

Mr. Vikas Kumar, Mr. Amit Tyagi, Mr. Amit Kumar
Assistant Professor, SRC,
Muzaffarnagar, UP., India

Abstract: ***MANET is a temporary set of connections in which nodes are moving without any fixed infrastructure or centralized supervision. The main characteristics of MANETs are: the complete lack of centralized control, lack of association among nodes, rapid mobility of hosts, frequent dynamically varying network topology, shared broadcast radio channel etc. There are many applications of MANET such as network-centric military/battlefield environments, emergency/rescue operations, disaster relief operations, intelligent transportation systems, fault-tolerant mobile sensor grids, environment control, and other security sensitive applications. In Mobile ad-hoc networks achieving security is even more challenging due to their specific properties. They have dynamic topology, no fixed infrastructure and the component devices have limited processing and battery power. There are many attacks affected to MANET such active and passive attacks. In this paper we introduce characteristics, Applications, Security issues, Challenges and Attacks in MANET.***

Keywords: Ad-hoc Network, MANET, Security, Challenges, Attacks etc.

I. INTRODUCTION

Mobile Ad hoc Networks are wireless network which are characterized by dynamic topology and no fixed infrastructure. Each node in a MANET is a computer that may be required to act as both a host and a router and, as much, may be required to forward packets between nodes which cannot directly communicate with one another. Each MANET nodes has much smaller frequency spectrum requirements that for a node in affixed infrastructure network [1]. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e. Routing functionality will be incorporated in to mobile nodes.

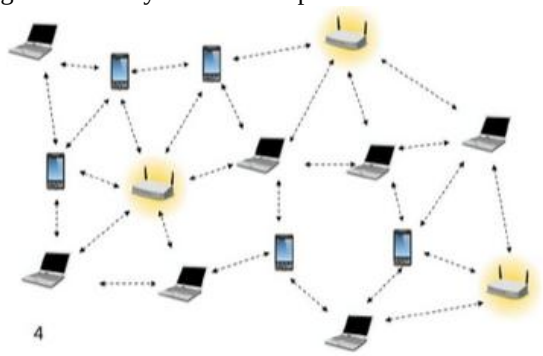

Figure 1 – MANET

Mobile ad hoc network got outstanding success as well as tremendous attention due to its self maintenance and self configuration properties or behavior. At early stage mostly people focused on its friendly and cooperative environment and due to this way many different problems came in being; security is one of the primary concerns in order to provide secure communication between different nodes in a mobile ad hoc network environment. The MANET has the following features :

- Dynamic network topology
- Bandwidth constraints
- Energy constrained nodes
- Multi hop communication
- Limited security
- Autonomous terminal
- Distributed operation
- Light-weight terminals

MANET is a type of multi-hop network, infrastructure less and the most important self-organizing [2]. Due to its wireless and distributed nature there is a great challenge for system security designers. In the last few years security problems in MANETs have attached much attention; most of the research efforts focusing on specific security areas, like securing routing protocols or establishing trust infrastructure or intrusion detection and response.

II. CHARACTERISTICS OF MANET

A MANET has the following characteristics [3]-

- In MANET, each node act as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

III. MANET LIABILITIES

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access [4][5]. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

1. Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

2. Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

3. Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

4. Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

5. Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

6. Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

7. Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

8. No predefined Boundary: In mobile ad- hoc networks we cannot precisely define a physical boundary of the network . The nodes work in a nomadic environment where they are allowed to join and leave the wireless network.

IV. MANET 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. 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. Typical applications include [6]-

1. 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.

2. 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.

3. 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.

4. 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.

V. SECURITY ISSUES

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner [7]. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

1. Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack [7].

2. Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

3. Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

4. Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key[7].

5. Non repudiation: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not[7].

6. Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

7. Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

VI. CHALLENGES IN MANET

Mobile ad hoc network has different challenges with respect to wireless security due to some of the following reasons:

1. The wireless network especially liable to attacks because of active eavesdropping to passive interfering.
2. Due to lack of Trusted Third Party adds, it is very difficult to deploy or implement security mechanisms.
3. Mostly Mobile devices have limited computation capability and power consumption functionalities which are more vulnerable to Denial of Service attacks. It is also incapable to run heavy security algorithms which need high computations like public key algorithms.
4. Due to MANET's properties like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words we need to cover up from both insider and outsider attacks in MANET, in which insider attacks are more difficult to deal with.
5. It is difficult to distinguish between stale routing and faked routing information because of node mobility mechanism. In node mobility mechanism it enforces frequent networking reconfiguration which creates more chances for attacks.

Below Table shows the security issues with respect to each layer .

S. No	Layer	Security Issues
1	Application Layer	In this layer we should prevent viruses, application abuses, worms, as well as malicious nodes.
2	Transport Layer	It provide authentication and provide secure end-to-end communications through data encryption between two nodes.
3	Network Layer	This layer deals with the protection of routing as well as

		forwarding protocols.
4	Link Layer	In this layer we mainly concern with the protection of wireless MAC protocol and also provide link-layer security.
5	Physical Layer	In this layer we should prevent signal jamming as well as denial-of-service attacks.

VII. MANET ATTACKS

The aims of Ad hoc networks and particularly MANET have in recent years not only seen widespread use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's range from simple wireless home and office networking to sensor networks and similarly constrained tactical network environments. Security aspects play an important role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks

7.1 Types of Attacks in MANET:

The current Mobile ad hoc networks allow for many different types of attacks. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly [8][9].

We have classified the attacks as modification, impersonation, fabrication, wormhole and lack of cooperation.

1. Attacks Using Modification

Modification is a type of attack when an unauthorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DoS attacks by modifying message fields or by forwarding routing message with false values [8]. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay.

2. Attacks Using Impersonation

As there is no authentication of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network.

3. Attacks Using Fabrication

The generation of false routing messages can be classified as fabrication attacks. Such attacks can be difficult to verify as invalid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted.

4. Wormhole Attacks

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

5. Lack of Cooperation

Mobile Ad Hoc Networks (MANETs) rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET gets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources.

VIII. CONCLUSION

In this paper we introduce MANET, characteristics, Applications, security issues, challenges in security and Attacks on MANETs. It is clear to us that due to the random mobility of node, security becomes a complex issue. Till now many security issues are used in MANET. The application layer has security issues for viruses, application abuses, worms, as well as malicious nodes. The transport layer has security issues for secure end-to-end communications through data encryption between two nodes. The network layer has security issues for protection of routing as well as forwarding protocols. The link layer has security issues for protection of wireless MAC protocol and also provide link-layer security.

REFERENCES

[1] https://www.scribd.com/doc/71867535/MC-Unit-7-MANET-s#scribd [2]. Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.

[2] Shuyao Yu, Youkun Zhang, Chuck Song, and Kai Chen. A security architecture for Mobile Ad Hoc Networks.

[3] http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/

[4] Weichao Wang, Yi Lu, Bharat K. Bhargava, "On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol", IEEE Proceedings, 2003, pp. 375-382

[5] Priyanka Goyal, Vinti Parmar and Rahul Rishi, *"MANET: Vulnerabilities, Challenges, Attacks, Application",* IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[6] Mohit Kumar and Rashmi Mishra "*An Overview of MANET: History, Challenges and Applications*" , Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[7] L. Zhou, Z.J. Haas, Cornell Univ., "*Securing ad hoc networks,"* IEEE Network, Nov/Dec 1999, Volume: 13, Page(s): 24-30, ISSN: 0890-8044

[8] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," *IEEE MILCOM*, 2002.

[9] Yi-an Huang and Wenke Lee. *"Attack analysis and Detection for Ad-hoc Routing protocols"*. Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France. September 2004.

