International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 09 | Sep 2018 www.irjet.net p-ISSN: 2395-0072

An Overview of MANET: Characteristics, Applications Attacks and Security Parameters as well as Security Mechanism

Reetu Singh

M.Tech, Dept. of Computer Science and Engineering, Galgotias University, Greater Noida, India

---

Abstract - *Presently a day, it is not any more optional to have security arrangements even unavoidable for each sort of organization and individuals. There are number of non-specific devices which are normal for organizations and additionally for individual clients to give security which incorporates; Anti-Spam, Anti-Virus and so on., and network security have turned out to be main issue in MANET. Security is one of the fundamental issues in the MANET particularly regarding size and complexity of the network. MANET is a sort of Ad Hoc connects with mobile, wireless nodes. Because of its unique attributes like dynamic topology, hop-by-hop communications and simple and fast setup, MANET faces so many difficulties symbolically routing, security and bunching. The security challenges emerge because of MANET's self-arrangement and self-support abilities. In this paper, we display some characteristics of MANET's , Applications of MANET's, Attacks in MANET layer wise some important parameters of MANET's as well as security mechanism of MANET's.*

Key Words: MANET, Characteristics, Applications, Attacks, Mechanism.

1. INTRODUCTION

MANET: A Mobile ad-hoc network (MANET) is wireless infrastructure which comprise of mobile nodes that are powerfully convey to each other over a wireless channel. Mo-bile ad-hoc network are combination of different wireless network like sensor net-work, cell network, which comprise of expansive number of mobile nodes. Nodes in MANETs can join and leave the system as per their necessities. In this network, there is no settled set of framework and centralized administration. The alterable idea of this kind of networks makes it very helpless to different connection attacks. The essential requirement for a secured networking is intense and secure routing protocol which guarantees the integrity of the network, confidentiality, availability and authenticity. Numerous past security answers for the wired networks are insufficient and wasteful for MANET environment. As the transmission happen in open medium system then it makes the Mobile ad-hoc network is more defenceless or vulnerable against security attacks. Different attacks can be reduced because of the availability of security protocols. In MANET speed differs as indicated by the applications, for e.g. in military application speed is quite low (long range network) yet in business application speed is quite high (short range network) i.e. network range is inversely prepositional to speed. Over the wireless system, it comprises two varieties of network infrastructure less and infrastructure. The infrastructure networks, in which mobile nodes associate with an entrance point like base stations that are associated with settled network infrastructure [1] [2]. The infrastructure less system is other kind of wire-less network, is knows as MANET. MANET has no settled access point while each node could be switch or host. MANETs lack central administration and prior organization, so security issues are different and in this way require different security mechanisms. Wireless interfaces in MANETs make it more inclined to the attacks for attackers. Attackers can specifically attack the web to erase messages, include malicious messages. In this paper, we will talk about various security issues and attacks of MANETS.

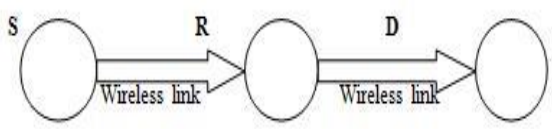

Fig 1: Ad-hoc networks S: Source, R: Router, D: Destination

1.1 Characteristics of MANET

Some characteristics are shown below [3]

- •self-arrangement and self-support abilities
- •All the nodes are mobile
- •Capabilities of network topology changes
- •Routing paths are variable
- •Dynamic topology
- •All the operations are distributed in nature
- •Fragmentation or decentralization
- •Scale variation
- •Energy constraint
- •Wireless Many hop routing

2. APPLICATIONS OF MANET

With the expansion of portable device and also advance in wireless communication, ad-hoc networking is picking up significance with the expanding number of across the board applications in the business, Military and private divisions. Portable Ad-Hoc Networks enable users to access and exchange data paying little mind to their geographic position or proximity of infrastructure [4] [5]. As opposed to the infrastructure networks, all nodes in MANETs are mobile and their associations are dynamic. Some applications of MANET is given below

- •military application
- •Wild life monitoring
- •Smart Agriculture

•Intelligent Transportation System
•Disaster Recovery

2.1 Military application

In comparison with geological situating frameworks, mobile ad-hoc networks can support the inherent geographical area by utilizing a to a great degree precise type of triangulation. This highlight enables soldiers in a military task to triangulate its position in view of the portable empowered vehicles or different devices. In mobile ad-Hoc networks, readings are quicker than the geographical situating frameworks in light of the fact that the soldiers don't need to wait for various satellites to get a centralized security. The devices use in battle tasks must have the capacity to address the two correspondences or communications security and an approach to secure the system from unauthorized access.

2.2 Wild life monitoring

Wild life Monitoring is important for storing details about the animal movement patterns. MANET's play very important role in this field with the help of MANET maintaining the track of wild life will become very simple and efficient. So many wild life acts are used to for monitoring [8].

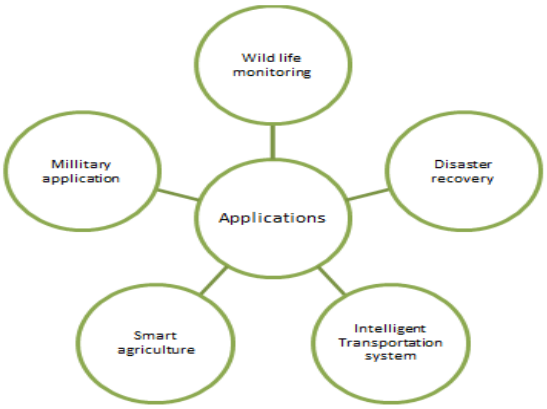

Fig 2: Applications of MANET's

2.3 Smart agriculture

To build the efficiency, created nations take after exactness agriculture. Exactness agriculture is to empower a quick and exact response to changes in natural conditions. It is made conceivable by inserting preparing devices in the checking area [6]. Wireless networks permit the organization of sensing systems and activation instruments at a significantly better level of granularity, and in a more mechanized usage than has been conceivable previously.

2.4 Intelligent transportation system

Road transportation system are generally characterized by how efficient they coordinate the traffic in non-congested way towards their goals or destinations. With the help of this application we maintain the traffic easily and efficiently.

2.5 Disaster recovery

With the help of different routing algorithm like as AODV, ZRP and OLSR MANET will play very important role in the field of disaster recovery [7]. MANET will use mobility modeling for maintaining its performance. With the help of MANET rescue teams will be efficiently communicate and coordinate with each other.

3. IMPORTANT PARAMETERS IN MANET SECURITY

In view of MANET's extraordinary qualities, there are some vital measurements in MANET security that are imperative in all security approaches; we call them "Security Parameters". Being unconscious of these parameters may cause a security approach pointless in MANET. Figure 3 demonstrates the connection between security parameters and security challenges [9]. Every security approach must know about security parameters as appeared in Figure 3. Security parameters in MANET are as per the following

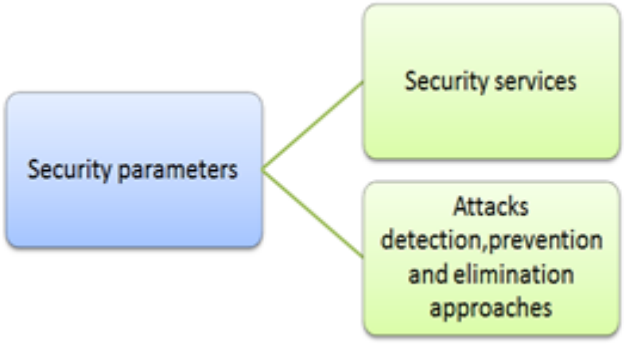

Fig 3: MANET security parameter

3.1 Network Overhead

This parameter alludes to number of control bundles produced by security approaches. Because of shared wireless media, extra control packets may effectively prompt congestion or collision in MANET. Packet lost is one the reply of congestion and collision. In this manner, high packet overhead builds packet lost and the quantity of retransmitted packets. This will simply wastes nodes vitality and network resources.

3.2 Processing Time

Each security approach needs time to recognize misbehavior and kill malicious nodes. Because of MANET's dynamic topology it's strongly possible that courses or routes between two unique nodes break because of mobility. Hence, security approaches must have as low as conceivable processing time keeping in mind the end goal to build MANET adaptability and abstain from rerouting process.

3.3 Energy Consumption

In MANET nodes have restricted energy supply. Subsequently, enhancing energy utilization is exceptionally challengeable in MANET. High energy utilization diminishes nodes and network's lifetime. Every security convention must know about these three essential parameters. In a few circumstances an exchange off between these parameters is given with a specific end goal to play out a fulfillment level in every one of them. Security protocols that carelessness these parameters aren't proficient as they waste network resources.

4. ATTACKS IN MANET

In MANET, there are various types of attacks which are performed by the attackers which are dependably attempts to decrease the execution of network. The Mobile Ad-hoc organize is more defenseless against different attacks not from outside but from inside the network itself. Securing wireless ad-hoc network is an exceedingly difficult issue. Understanding possible type of attacks is dependably the initial move towards growing great security arrangements. Security of communication in MANET is imperative for secure transmission of data [10] [11] [12]. Nonappearance of any focal co-appointment component and shared wireless medium makes MANET more helpless against cyber/digital attacks than wired networks there are various attacks that influence MANET. These attacks can be named in the following table:

Table -1: Attacks in MANET layer [2]

MANET LAYER	TYPES OF ATTACKS ON LAYERS
Application Layer	Malicious code, Repudiation
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Flooding, Black Hole, Grey Hole , Worm Hole, Link Spoofing
Data link Layer	Traffic analysis and monitor
Physical Layer	Eavesdropping, jamming

4.1 Application layer attacks

Malicious code attacks

Malicious code attacks incorporate Worms, Viruses, Trojan horse and Spywares can attacks both operating system and client application.

Repudiation attacks

Repudiation refers to a denial of cooperation or participation in all or part of the interchanges or communications. Huge numbers of encryption system and firewalls utilized at various layer are not adequate for packet security.

4.2 Transport layer attacks

Session Hijacking

Attacker in session hijacking takes the favorable position to abuses the unprotected session after its underlying or initial setup. In this attack, the attacker spoof the victim node's IP address, finds the right sequence number i.e. expected by the objective and after that dispatches different DOS attacks. In Session hijacking, the malicious node attempts to gather secure information (passwords, secret keys, logon names and so forth.) and other data from nodes. System and firewalls utilized at various layer are not adequate for packet security.

SYN Flooding Attack

The SYN flooding attacks are the kind of Denial of Service (DOS) attacks, in which attacker makes countless half opened TCP connection with victim node. These half opened connection are never finishes the handshake to completely open the connection.

4.3 Network layer attacks

Flooding attack

In flooding attack, attacker debilitates the network resources, for example, data transfer capacity and to consume a network resources, for example, computational and battery control or to interrupt the routing operation to cause serious degradation in network execution. For instance, in AODV protocol, a malicious node can send so many numbers of RREQs in a very short period to a receiver node that does not exist in the system or network. Since nobody will answer to the RREQs, these RREQs will flood the entire network.

Black hole Attack

Route searching process in AODV is vulnerable to the black hole attack. The technique, that is, any intermediate routing node may react to the RREQ message, if it has so many fresh routes formulated to reduce routing delay, is utilized by the malicious node to trade off the system. In this attack, when a malicious node tunes to a route request packet in the system, it reacts with the claim of having the most limited and the freshest route to the receiver node regardless of whether no such route exists.

Wormhole Attack

In a wormhole attack, an attacker gets packets at one point in the network, "tunnels" them to another point in the system, and after that replays them into the system starting there. Routing can be affected while routing control message are tunnelled. This tunnel between two conniving attacks is known as a wormhole .In DSR, AODV this attack could avoid

searching of any routes and may make a wormhole even for packet not deliver to itself due to broadcasting.

Grey hole attack

This attack is otherwise called routing trouble making attack which prompts drop-ping of messages [13]. Grey hole attack has two stages. In the principal stage the node promote itself as having a valid route to receiver while in second stage, nodes drops captured packets with a specific probability.

Link spoofing attack

In a Link spoofing attack, a malicious node promotes fake connections with non-neighbours to disturb routing tasks. For instance, in the OLSR protocol, an attacker can publicize a fake connection with a goal's two hop neighbours. This makes the goal node to select the malicious node to be its MPR. As a MPR node, a malicious node would then be able to control information or routing movement, for instance, changing or dropping the routing traffic or performing different kinds of DOS attacks.

4.4 Data link layer attack

Traffic Analysis

In MANETs the information packets as well as traffic design both are important for publicity. For instance, private information about network topology can be develop by analyzing traffic design [14]. Traffic analysis can also be organize as dynamic attack by destroying nodes, which stimulates self-association in the network, and profitable data about the topology can be assembled.

Traffic monitoring and analysis

Traffic monitoring and analysis can be conveyed to distinguish the communication parties and functionalities, which could give data to dispatch further attacks. Since these attacks are not particular to the MANET, different wireless systems, for example, the cell network, satellite network, and WLAN likewise experience the ill effects of these potential vulnerabilities.

5. Physical layer attack

Eavesdropping

This is a type of passive attack. The node essentially watches the confidential data [15]. This data can be later utilized by the malicious node. The secret data like area, public key, private key, password and so forth can be fetched by eavesdropper.

Jamming

Jamming is a special or exceptional class of DOS attacks which are started by malicious node subsequent to deciding the frequency of communication. In this kind of attack, the jammer transmits signals alongside security threats. Sticking attacks likewise keeps the gathering of real packets.

5. SECURITY MECHANISM IN MOBILE AD-HOC NETWORK

Generally there are two types of security techniques in MANET, which are secure routing techniques and intrusion detection. Intrusion detection is again divided in two parts [16].

5.1Intrusion Detection

AN Intrusion Detection System (IDS) is an essential a part of a security system and is specially introduced to observe potential violations of the safety policy by watching system activities and responding to people who area unit apparently intrusive [17]. If an attack is detected once within the network, a response is initiated to avoid or curtail the injury to the system.

Misuse-based Intrusion Detection

Misuse-Based IDSs detection attack signatures with current network activities. They're usually most popular by industrial IDSs since they're economical and have a very low false positive rate. The most disadvantages is that it cannot observe new at-tacks. There's a necessity for frequent change of data, since the system is barely as robust as its signature data.

Anomaly-based intrusion Detection

It detects intrusions as anomalies, i.e. deviations from the conventional behavior patterns. The conventional activities that area unit detected as anomalies by IDS may be high in anomaly-based detection and additionally, it's capable of searching unknown attacks.

5.2 Secure routing

A Secure spontaneous Routing Approach exploitation localized Self-healing Communities

Self-healing community is beneficial only if there's a minimum of one cooperative "good" node within the community. Many routing techniques facilitate in creating secure the spontaneous routing security. A number of them influence specific attacks that aim to disturb the spontaneous routing services, give and supply some solutions to assist defend against these attacks whereas alternative techniques try and provide some effective tools or schemes to safeguard the spontaneous routing services from all types of attacks.

6. CONCLUSIONS

The aim of this paper is to know the goals , parameters , security mechanism , Characteristics , attacks and applications of MANET so as to encourage the research work in this field[18][19]. During the detail study of MANET we

are able to know that Mobile Ad-hoc Networks we are expected to be very useful and important framework for achieving future ubiquitous society. MANET framework is dynamic in nature and having decentralized administration that makes this system is more vulnerable to many attacks. In this paper we define the attacks layer wise.

REFERENCES

[1] International Journal of Computer Science and Mobile Computing IJCSMC, A Review: Security Issues in Mobile Ad Hoc Network Priti, Dr. Priti Sharma

[2] International Journal of Computer Science and Mobile Computing an Overview of MANET: Applications, Attacks and Challenges 1Mr. L Raja, 2Capt. Dr. S Santhosh Ba-boo.

[3] International Research Journal of Advanced Engineering and Science ISSN Review Paper on Security Issues in Mobile Adhoc Networks Vikas Goyal, Geeta Arora

[4] International Journal of Application or Innovation in Engineering & Management (IJAIEM) MANET: History, Challenges And Applications Ankur O. Bang, Prabhakar L. Ramteke.

[5] Security Issues in Mobile Ad Hoc Network Noman Islam1 and Zubair Ahmed Shaikh2.

[6] Quality Enhancement of Agricultural Industry using MANETS R. Sivakami, Dr.G.M. Kadhar Nawaz.

[7] African Journal of Computing & ICT Mobile Ad-Hoc Network Performance in a Disaster Management Scenario A. Srivastava, D. Kumar & S.C. Gupta Department of Electrical Engineering, Indian Institute of Technology (BHU).

[8] Smart Computing and Sensing Technologies for Animal Welfare: A Systematic Review Admela Jukan, Xavi Masip-Bruin and Nina Amla.

[9] International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015 Security Challenges In Mobile Ad hoc Networks: A Survey Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah Department of Computer Engineering, Mashhad branch, Islamic Azad University, Mashhad, Iran.

[10] Krishna Moorthy Sivalingam, "Tutorial on Mobile Ad Hoc Networks", 2003.

[11] "THE HANDBOOK OF AD HOC WIRELESS NETWORKS" Edited by Mohammad Ilyas Florida Atlantic University Boca Raton, Florida

[12] Ad hoc network specific attacks held by Adam Burg.

[13] J.Sen, B. Tata, M. Chandra, S. Harihara, and H. Reddy, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks," presented at the 6th International Conference on Information, Communications & Signal Processing, 2007

[14] Wu B., Chen J., Wu J., Cardei M., "A Survey on Attacks and Countermeasures in Mo-bile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12, Springer, 2006

[15] The Hand book of AdHoc Wireless Networks (chapter 30), CRC press LLC, 2003.

[16] 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016) Security Issues In Mobile Ad Hoc Networks Sarika S, Pravin A, Vijaya-kumar A , Selvamani K.

[17] P.Yi, X. Jiang, and Y. Wu, "Distributed intrusion detection for mobile ad hoc net-works," Journal on Systems Engineering and Electronics, IEEE.

[18] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester " An Overview of Mo-bile ad hoc Netwroks: Applications & Challenges.

[19] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and chal-lenges. Ad Hoc Network.

AUTHOR

Reetu Singh Student of M.tech (Computer Science and Engineering) of Galgotias University Greater Noida, INDIA. Done B.Tech in Computer Science and Engineering.