Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 2; January-March, 2015 pp. 167-172

http://www.krishisanskriti.org/acsit.html

MANET: Mobile Ad-hoc Network its Characteristics, Challenges, Application and Security Attacks

Neha Yadav[1] and Divya Sharma[2]

[1]Student ITM University Gurgaon
[2]ITM University Gurgaon
E-mail: [1]rs.nehayadav21@gmail.com, [2]divya@itmindia.edu

Abstract— *A wireless ad-hoc network is a new decentralized style of Wi-Fi multilevel. The network is called ad-hoc because it doesn't rely on pre-existing infrastructure like routers inside "cable " CPA networks. An ad hoc network is a group of wireless mobile hosts combine to complete a momentary circle with no aid of any centralized administration. Due to limited distribution selection of every cell host's in wireless transmission this type of environment is helpful for a single mobile host to enroll and help other nodes in forwarding a packet to its destination .*

Ad hoc networks often have mobile nodes, which also implicates that they apply wireless communication to maintain the connectivity, in which case the networks are called as mobile ad hoc networks (MANET). Many attempts have been made to use traditional routing methodologies with regard to routing throughout random

Networks, healing each portable web host as a router. This paper discusses about mobile ad-hoc network (MANET) and its characteristics, challenges, application, security goals and different type's security attacks at different layers of TCP/IP model.

1. INTRODUCTION

Mobile ad-hoc network (MANET) is a type of ad-hoc network, likewise ad-hoc networks MANETs also have random wireless nodes moving freely in the wireless domain. MANET is a self organized system consists of mobile wireless nodes .In MANET all nodes act as both communicators and routers. MANET present fast and simple deployment associated with multilevel throughout conditions in which it's not possible or else. MANET is usually most suitable choice with regard to m services in which there's no predefined structure. MANET has a wide range of applications ranging from everyday mobile phone application to mission, critical military applications. MANETs have proved their certainty and the ease of setting up networks, thus MANETs are very popular for frameworks which are sensitive and urgent like emergency services, military battlefield network etc. Because of the ad hoc nature MANETs are usually prone to safety measures attacks. MANETs consist of wireless mobile nodes that dynamically self organized in inconsistent and temporary network topologies. In MANETs nodes can directly communicate with all the other nodes within their radio ranges where as nodes that are not in the direct communication range use intermediate nodes to communicate with each other. For example, Fig. 1 illustrates an easy ad-hoc system associated with several cellular nodes using wireless system interfaces. Number C is just not from the range of number A's wireless transmitter (indicated because of the group close to A) as well as number A is just not from the range of C's wireless transmitter. In the event that node A as well as node B would like to change packets, they might however enlist the providers associated with number B to help forward packet's for the kids. Considering that B is at the overlap between A's selection as well as C's selection. The formatter will need to create these components, incorporating the applicable criteria that follow.

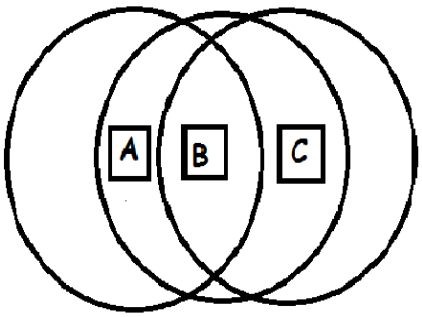

Fig. 1: Mobile ad-hoc network

1.1. Characteristics of MANETS

Some of the MANETs characteristics are:

1) Distributed operation: There is no structure community for the middle handle from the community functions; your handle from the community has been allocated one of the nodes. The actual nodes associated with any MANET need to closely with jointly in addition to converse jointly, for you to apply unique capabilities for instance redirecting in addition to protection.

2) Multi hop routing: Whenever a node endeavors for you to mail info for you to some other nodes that are outside of its conversation range, your bundle must be submitted through number advanced nodes.

3) Autonomous terminal: Throughout MANET, almost any cell node can be an neutral node, which can really do the a couple of such as a mentor as well as a router.

4) Dynamic topology: Nodes are liberal to go with little thought with unique rates, thus the particular multilevel topology may well transform at random, as well as in unforeseen time. Your nodes within the MANET dynamically establish redirecting involving themselves when they take a trip around, creating their own network.

5) Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU capability, low power, storage and small memory size.

6) Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

7) Network Scalability: Now days, common network management algorithms were principally designed to Fig. on fastened or comparatively little wireless Many mobile unintentional network programs involve substantial communities at the side of thousands of nodes, as found for instance, in sensing element networks and Tactical networks. Measurability is essential to the thriving readying of those networks. The steps toward an oversized network consisting of nodes with Limited resources don't seem to be easy, and located several problems that are not withstanding for being fastened. In areas such as: addressing, routing Location management, configuration management, ability, security, high capability wireless technologies, etc.

1.2. Application of MANETs

Some of the typical applications include:

1) Military battlefield: Ad-Hoc networking would allow the actual military to help make the most of typical area system technological know-how to maintain a great data system between the members of the military, automobiles, in addition to military data scalp Quarter.

2) Collaborative function: For some organization circumstances, the necessity pertaining to collaborative processing may be more crucial outdoors business office circumstances than inside of and exactly where people accomplish require outdoors conferences to be able to interact personally and swap information on a given undertaking.

3) Local level: Ad-Hoc networks can autonomously hyperlink an instantaneous and also momentary hibernal network employing mobile computing to help distributed and also share info among contributors, e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

4) Personalized area as well as Wireless bluetooth: A personal place community is usually a limited collection, nearby process the place nodes will often be of your granted individual. Short-range MANET for example Wireless bluetooth may simplify the inter transmission involving numerous cellular devices say for example a notebook, and a mobile phone.

5) Commercial Field: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency relief operations need to be held where by non-existing or maybe harmed communications commercial infrastructure along with fast deployment of the connection circle is needed.

2. MANET CHALLENGES

Despite of the variety of applications and the long history of mobile ad hoc network, there are still some issues and challenges that we have to overcome. This is the reason MANET is one of the elementary research field. MANET is a wireless network of mobile nodes it’s a self organized network. Each system can certainly interact with some other system i.e. it is also multi hop network.

As it's a cellular circle it inherits the traditional problem associated with cellular social networking that are next:

1) The channel has time fluctuating and unbalanced spread properties.

2) The wireless media is less or not reliable as compared to the wired media.

3) Invisible terminal and present terminal sensation may possibly occur.

4) The channel is not protected from outside signal Main title.

With one of these issues there are numerous some other challenges and also difficulties arise. The scalability is required in MANET as it is used in military communications, because the network grows according to the need, so each mobile device must be capable to handle the intensification of network and to accomplish the task. MANET is an infrastructure less network, there is no central administration. Each device can communicate with every other device, hence it becomes difficult to detect and manage the faults. In MANET, the mobile devices can move randomly. The use of this dynamic topology results in route modifications, recurrent circle partitions and maybe box failures.

Each node in the network is autonomous hence has the equipment for radio interface with different transmission/ receiving capabilities these results in asymmetric links. MANET uses no router in between. Throughout the network each and every node operates as being a router which enables it to. and can forward packets of data to other nodes to provide information partaking among the mobile nodes.

3. SECURITY: IMPORTANCE, GOALS AND ATTACKS

Before the provision of security services in MANET is dependent on the characteristics of the supported application and the networked environment, which may vary significantly in mobile ad hoc networks, security depends on several parameters (authentication, Confidentiality, integrity, availability and non-repudiation) without one of these parameters, security will not be complete.

Authentication: Every node which sends or receives the message packets has its own signature. These nodes must be able to authenticate that the data has been sent by the authorized node. Authentication is defined as the conformation of statements regarding the personality of the cause of info. Authenticity is important to assure that the participants with transmission are generally authentic rather than impersonators. To guarantee the authenticity it is vital with the transmission participants to help prove their particular identities while precisely what they've said using some methods. Devoid of authentication, the enemy can masquerade as being a node, thus getting unauthorized usage of reference and also vulnerable data interfering using the procedures of the different nodes.

Confidentiality: It means that only authorized people or systems can read or execute protected data or programs. It should be noted that the sensitivity of information in MANETs may decay much more rapidly than in other information. Only the intended receivers should be able to interpret the transmitted data.

Integrity: Data should not change during the transmission process, i.e., data integrity must be ensured Means that the information is not modified or corrupted by unauthorized users or by the environment. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised in two ways malicious altering and Accidental altering.

Availability: It refers to the ability of the network to provide services as required. The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it.

Non-Repudiation: Ensures that committed actions cannot be denied. It can be explained as sender of a message shall not be able to later deny sending the message and likewise recipients shall not be able to deny the receipt after receiving the message.

Being exposed is usually a weakness inside security technique. A specific technique may be at risk of unauthorized facts manipulation for the reason that technique won't confirm the owner's identity before enabling facts access. MANET will be a lot more vulnerable when compared with wired networks. Many of the vulnerabilities are usually the following:

Insufficient centralized management: MANET does not have a centralized track of server. The particular lack of administration tends to make the particular discovery associated with episodes complicated simply because it's not at all simple keep track of the particular site visitors inside a hugely active in addition to big range ad-hoc system.

- Simply no predefined Boundary: Inside mobile ad- hoc communities (MANET), all of us are unable to determine a real border in the network. This nodes perform within open up setting in which these are permitted to enroll in and also abandon this wifi network. When a good enemy also comes in the air variety of a node the item are able to contact of which node also.
- Cooperativeness: Redirecting algorithm intended for MANETs usually takes on that nodes are cooperative and also non-malicious. As a result destructive actions, attacker can just grow to be a necessary direction-finding adviser and also impact community procedure.
- Limited power supply: There exists a restricted power supply throughout portable ad-hoc system, which in turn will result in various difficulties. Getting some sort of node throughout portable ad-hoc system may possibly work inside a self-centered tactic if it's locating there's solely confined strength.
- Enemy inside the Network: The particular cell phone nodes within the MANET can openly become a member of along with depart your system. The particular nodes within just system can also behave maliciously. This can be tough for you to diagnose how the conduct of the node is actually malicious. So this kind of invasion is actually much more risky compared to outer invasion.

Securing wireless ad hoc network can be a very demanding issue. Ad hoc networks ought to address similar varieties of vulnerabilities as ancient networks, yet like new vulnerabilities specific to the unplanned context.

4. SECURITY ATTACKS

The security threats detected by MANETs is the extension and expansion of that be confronted by wired network in the wireless fields, which mainly comes from wireless channels and networks. The particular threats can be portioned into a

couple of groups passive along with active attacks. Active attacks involve actions such as the replication, modification and deletion of exchanged data. Certain active assaults might be very easily executed next to a good ad hoc network. These attacks can be defined as: Impersonation, Denial of service, and Disclosure attack. Fig. (2) explains the various attacks in MANETs.

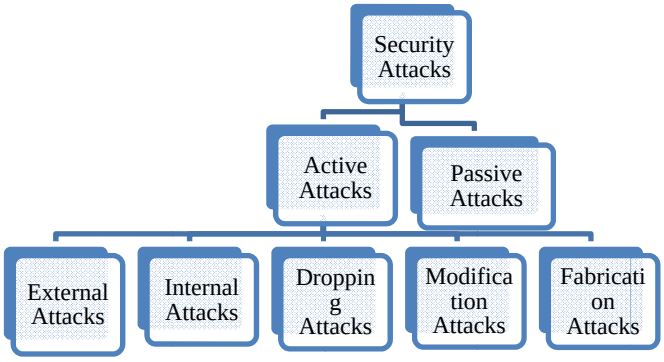

Fig. 2: Explanation of Security Attacks in MANET.

4.1 Passive attacks: 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.

4.2 Active attacks: 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. Active Internal attacks are from malicious nodes which are part of the system, internal attacks are more critical as well as hard to detect when compared with external attacks. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DOS, congestion etc.

Active attacks are however further classified into three groups:

Dropping Attacks: Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes.

- Modification Attacks: These attacks modify packets and disrupt the overall communication between network nodes. Sinkhole attacks are the example of modification attacks.
- Fabrication Attacks: In fabrication attack, the attacker send fake message to the neighboring nodes without receiving any related message. The characteristics of MANETs make them susceptible to many new attacks.

These attacks can occur in different layers of the network protocol stack.

4.2.1. Attacks at Physical Layer: Attacks found at physical layer are eavesdropping, Active interference, and jamming etc.

- Eavesdropping: It can also be defined as interception and reading through messages and conversations through unintentional receivers. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication.
- Jamming: Jamming is a special class of Denial of service (Dos) attacks which are initiated by malicious node after determining the frequency of communication. Jamming attacks also prevents the reception of legitimate packets.
- Active Interference: An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications.
- Malicious message injecting: These kinds of attacks are happened from compromised entities or stolen device like physical capturing of a node in MANET.
- Stolen or Compromised Attack : Attacker inject false streams into the real message streams which is routing through the intermediate nods, due to malicious message injecting the functionality of network is disrupted by the attacker.

4.2.2 Attacks at Data link layer: Some of the attacks identified at data link layer are:

- Selfish Misbehavior of Nodes: The selfish nodes may refuse to take part in the actual forwarding procedure or perhaps declines the actual packets, intentionally in order to conserve the resources and to conserve of battery power.
- Malicious Behavior of nodes: The main task of involving harmful node should affect usual operations involving routing project. This influence involving like attack can be improved if the communication occurs concerning border nodes. Assaults involving like form are usually belonging to next different types. Attacking neighbor realizing protocols: malicious nodes promote artificial error announcements in order that significant back links software and are noticeable seeing that shattered.

4.2.3. Attacks at Network Layer: some of the network layer attacks are

- Black hole Attack: In this type of attacks, malicious node claims having an optimum route to the node whenever it receives RREQ packets, and sends the REPP with highest

destination sequence number and minimum hop count value [1] to originator node whose RREQ packets it wants to intercept. Almost all

- packets are usually dropped simply by delivering solid redirecting packets, the attacker may course many packets for a few location to be able to alone after which dispose of them, or maybe the attacker might cause the course in any respect nodes within an section of the system to be able to place in which area whenever in reality the location will be beyond your area.
- Sinkhole Attack: In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving whole network traffic it modifies the secret information, such as changes made to data packet or drops them to make the network complicated. A malicious node tries to attract the secure data from all neighboring nodes.
- Link Spoofing Attack: Within a web page link spoofing assault, destructive node states phony hyperlinks using non-neighbors to be able to disturb redirecting surgical procedures. A good attacker can certainly advertise a phony web page[8] link with a target's two-hop neighbors. This specific brings about the prospective node to choose your destructive node for being the multipoint exchange node (MPR).
- Message fabricating: In this kind of attack false stream of messages is added into information which is communicated or some kind of change is done in information.
- Route Tracking: This kind of attack is done to obtain sensitive information which is routed through different intermediate nodes.

4.2.4 Attacks at Transport Layer

- Session Hijacking: Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial setup. In this attack, the attacker spoofs the victim node's IP address, finds the correct sequence number i.e. expected by the target and then launches various DOS(denial of service) attacks.
- Jelly Fish Attack: The attacker disrupts the TCP connection which was established for communication. A jelly fish attacker needs to intrude into [10]forwarding group and then it delays info packets unnecessarily for some amount of time just before ahead all of them. Due to this attack a high end to end delay & delay jitter is happened. So the performance of real time applications becomes worst.
- TCP SYN Attack: TCP SYN attack is DOS(Denial of service) in nature, so the legitimate user does not get the service of network when attack is happened. TCP SYN attack is performed by creating a large no of halt in opened TCP connection with a target node.
- TCP Session Hijacking: TCP session hijacking is done by the spoofing of IP address of a victim node after that attacker steals sensitive information which is being communicated. Thus the attacker captures the characteristics of a victim node and continues the session with target.

4.2.5. Attacks at Application Layer

- Malicious code attacks: This type of attacks includes, Viruses, Worms etc however they can attack both operating system and user application.[1]
- Repudiation attack: Due to repudiation attack deny of participation is happened in whole communication, or in a part of communication.
- Attacks by Worms and Virus: Attack is done by virus, worms to infect the operating system or application software installed in mobile devices.[5]
- Denial of Service (DOS): The prevention of certified usage of sources as well as the particular slowing down connected with time-critical operations. A refusal connected with service (DOS) episode is actually seen as a shot through an assailant to avoid reputable consumers of a service from while using the sought after sources as well as efforts to help "flood" some sort of multilevel, therefore avoiding reputable multilevel traffic.
- Misdirecting traffic: A new harmful node advertises inappropriate redirecting data in order to get secure information prior to the precise route.

Table 1: Attacks corresponding to different layers of TCP/IP model.

TCP/IP LAYER	TYPES OF ATTACKS
Physical Layer	**1 Jamming, 2 Active Interference, 3 Eaves Dropping, 4 Stolen or Comprised attack, 5 Malicious messages injecting.**
Data Link Layer	**1 Selfish misbehavior of nodes, 2 Denial of service, 3 Malicious Behaviors of nodes , 4 Misdirecting traffic , 5 Attacking neighbor sensing protocols .**
Network Layer Attack	**1 Black hole Attack , 2 Rushing Attack , 3 Wormhole Attack , 4 Grey hole attack ,5 Sinkhole Attack , 6 Message Fabricating , 7 Route Tracking , 8 Link Spoofing Attack**
Transport Layer	**1 Session hijacking, 2 jelly Fish Attack, 3 TCP SYN Attack, 4 TCP Session Hijacking.**
Application Layer	**1 Malicious code attack, 2 Repudiation attack, 3 Attacks by virus and worms.**

5. CONCLUSION

This paper gives an overview of mobile ad-hoc network and its challenges related to attacks held on each layer of the network protocol stack (TCP/IP model). This paper also includes a hierarchy of MANETs routing protocols and a

comparison table of attacks, corresponding to the different layers of TCP/IP model.

REFERENCES

[1] S.adibi , G.B.Agnew “Multilayer flavoured dynamic source routing in mobile ad-hoc networks” IET communication on 6,March 2007.

[2] Baljeet Kaur “Security Architecture for MANET and it’s application in m-governance” International conference on communication systems and network Technologies”, 2013.

[3] X.Li,Z.Jia,P.Zang,R.Zhang,H.Wang “Trust Based on-demand multipath routing in mobile ad-hoc networks “ IET Information Security 1,August, 2009.

[4] N.Marchang , R.Datta “Light Weight Trust-based routing protocol for mobile ad-hoc network” IET Information Security July,2010 .

[5] R.Venkataraman , M.Pushpalatha , T. Rama Rao “ Regression based trust model for mobile ad hoc networks “ IET Information Security August,2011.

[6] Hideshia nakayama , Member,IEEE , Satoshi Kurosawa,Abbas Jamalipour,Fellow,IEEE,Yoshiaki Nemoto , Senior Member ,IEEE and Nei Kato,Senior Member ,IEEE “ A Dynamic Anomaly Detection Scheme for AODV based Mobile Ad-Hoc Networks “IEEE Transaction on Vehicular Technology Junes,2009.

[7] Alex Hinds, Michael Ngulube , Shaoying Zhu and Hussain Al-Aqrabi “ A Review of Routing Protocols for Mobile ad-hoc network (MANET)” International Journels of Information and Education Technology ,Vol 3, No. 1, Feburary 2013.

[8] Lidong Zhou , Zygmunt J Securing ad-hoc networks ,Cornell University Ithaca, NY 14853.

[9] Deepak Chayal, Dr. Vijay Singh Rathore “ASSESSMENT OF SECURITY IN MOBILE AD-HOC NETWORKS (MANET)” Volume 2, No. 6, June 2011 Journal of Global Research in Computer Science.

[10] Durgesh Wadbude, Vineet Richariya “An Efficient Secure AODV Routing Protocol in MANET” International Journal of Engineering and Innovative Technology (IJEIT)Volume 1, Issue 4, April 2012.

[11] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, & E. Belding-Royer,” A secure routing protocol for ad hoc networks” Proc. 10th IEEE International Conference of. Network Protocols (ICNP ’02), 2002, 78–87.

[12] M. Zapata, N. Asokan, “Securing ad hoc routing protocols” Proc. ACM Workshop on Wireless Security (WiSe), 2002, 1–10.

[13] Asad Amir Pirzada and Chris McDonald “Secure Routing with the AODV Protocol” Asia-Pacific Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.

[14] Radha Krishna Bara,Jyotsna Kumar Mandalb and Moirangthem Marjit Singh “QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack” International Conference on Computational Intelligence: Modeling Techniques and Applications CIMTA) 2013.