International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Review on MANETs Characteristics, Challenges, Application and Security Attacks

Anuj Rana[1], Sandeep Gupta[2]

[1]M. Tech (CSE), Hindu College of Engineering, Sonipat, Haryana, India

[2]Assistant Professor (CSE), Hindu College of Engineering, Sonipat, Haryana, India

Abstract: ***Mobile ad hoc networks (MANETs) are wireless, un-infrastructure, dynamically linked network consists of a collection of wireless mobile nodes that communicate with each other without centralized monitoring & Control. These fundamental characteristics, such as wirelessly connecting medium, dynamic natured topology used, distributed cooperated network. MANETs are vulnerably natured to various kinds of security related attacks such as wormhole attacks, greyhole attacks, rushing attacks, blackhole attacks. This paper review about mobile ad-hoc networks, its characteristics, challenges faced, applications, security related goals and different types of attacks.***

Keywords: Wireless Ad-hoc Networks, MANETs, Routing Protocols & Attacks.

1. Introduction

Now a days the fastest developing technologies and internet networks, accessible for everyone, where there are no clear boundaries between the functionality of the "gadgets" and the possibility to communicate is not an option but necessity, the mobile ad hoc networks (MANETs) plays significant role. A mobile ad hoc network (MANET) (Figure 1) is a dynamic self-configuring wireless network of mobile devices, in which every single node can act as router. This router can possess multiple hosts and wireless devices. These devices are freely moving arbitrarily as a result they can interact with each other though there is no strictly defined structure or centralized administration [6], using wireless connections. These networks are fully distributive and can be freely works at any place without taking help of any fixed infrastructure and provide access points or base stations. The figure shown below is basic simple ad-hoc network having mobile nodes.

Figure 1: Example of mobile ad-hoc network

A. MANETs Characteristics

1) *Distributed operation*: There is no background network for the central control of the network operations. The nodes control over the network is distributed. The nodes should cooperate with each other and communicate among themselves also each node acts as a router if required it also includes specific functions such as routing as well as security.
2) *Multi hop routing*: When a node tries to send information to other nodes which is out of its communication range, then *the* packet should be forwarded via relay of intermediate nodes.
3) *Autonomous terminal*: MANETs are those networks in which each mobile node is independent node, which function as both a host and a router.
4) *Dynamic topology*: Nodes are free to move arbitrarily in any direction with different momentum speed therefore network topology changes randomly and on unpredictable time. The MANET nodes or devices on runtime establishes routing among themselves as they travel around, establishes their own network.
5) *Light-weight terminals*: In maximum cases, the nodes in MANETs are mobile having less CPU capability, having low power storage and less memory size.
6) *Shared Physical Medium***:** The wireless medium of communication is reachable to any entity with the equipment that is appropriate and having adequate resources. Hence accessing to the channel cannot be restricted.

B. Advantages of MANET

The advantages of Mobile Ad-Hoc networks are as following [3]:

- Regardless of geographic position MANETs provide access to information as well as services.
- Because of Self-configuring networks, MANETs are independent from central network administration. Nodes are also act as routers. They are less expensive than wired network.
- Scalability feature provides accommodation for addition of more nodes.
- They have highly improved Flexibility.
- They are robust due to decentralized administration.
- The network can easily be set up at any of the place and time.

C. MANETs Challenges

1)*Limited bandwidth*: They have wireless link so that it continue to have notably lower capacity than infrastructure networks. In accounting for the effects of several times access, fading, sound, and interference conditions are realized to be the throughput of wireless communication

often much less than a radio's maximum transmission rate.

2) *Dynamic topology*: It may disturb the trust relationship among nodes due to Dynamic topology membership. This trust also is disturbed if considerable nodes are detected to be compromised.
3) *Routing Overhead*: In mobile adhoc networks, nodes may be habitually change their location over the network. So, it leads to unnecessary routing overhead due to some stale routes generation in the routing table.
4) *Hidden terminal problem***:** The name suggests, the hidden terminal problem also referred as the crash of packets at a receiver node due to the simultaneous transmission by these nodes that should not be within direct transmission range of sender in spite of within the transmission range of the receiver.
5) *Packet losses due to transmission errors*: The mobile Ad hoc wireless networks practiced a much higher packets loss by means of factors such as increased collisions within the presence of hidden terminals also in .presence of interference, uni-directional links & repeated path breaks due to mobility of nodes.
6) *Mobility-induced route changes*: Due to dynamic topology of an ad hoc wireless network, it is highly dynamic in nature due to the movement of nodes. Hence the on-going session also suffers from regular path breaks. This underlying situation mostly leads to frequent route changes.
7) *Battery constraints*: Battery containing Devices are used in these networks. Hence they have restrictions on the power source for maintaining portability, its size and weight of the device.
8) *Security threats*: Many new security challenges to the network design provided by wireless mobile ad hoc nature of MANETs. The wireless medium is heavily vulnerable to eavesdropping and mobile ad hoc network functionality. The mobile ad hoc network functionality is done through node cooperation, between mobile ad hoc networks. These are intrinsically exposed to numerous security attacks.

D. MANETs Applications

Few Important applications of MANETs are:

1) *Military battlefield:* MANETs provide us to allow the military for maintaining information about network in between the soldiers, vehicles also in military information head quarter provides an advantage of commonplace network technology.
2) *Commercial Sector*: Mobile Ad hoc networks can also be used within emergency rescuing operations for disaster management and relief efforts like in floods, or volcanic conditional activities also in fires. It also helps in emergency rescuing operations must also take place where there is either non-existing or damaged communicational infrastructure or needs of rapid deployment of a communication network required.
3) *Collaborative work: S*ome business environment might needs joint computing might be more significant outside office environmental conditions than inside environmental conditions where people do require providing outside meetings for cooperation and exchanging information on project.
4) *Local level:* Mobile Ad-Hoc networks are autonomously linked an instantaneous and temporal multimedia network by using portable computers also to spread and sharing information among members at a e.g. meeting or conference. Another most appropriate locally leveled application within home networks where nodes can communicate directly for exchanging information.
5) *Personal area network and Bluetooth:* A simple personal area network is a small ranged and localizing network in which nodes are usually associated with a given person. MANETs that are short-ranged like Bluetooth network can simplify the inter communication between various mobile devices such as a personal laptop and any device that is mobile.

2. MANETs Vulnerabilies

Vulnerability also refers as weak spot in any system that is secure. Most of the systems are vulnerable toward data manipulation if it does not verify user identification before allowing to unauthorized access. As compared to wired network mobile ad-hoc networks are more vulnerable. Vulnerabilities of mobile ad-hoc networks are as follows [10]:

1) *Lack of centralized management*: MANETs doesn't have a centralized server for monitoring. 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.
2) *No predefined Boundary*: No boundary is defined in Mobile Ad-Hoc networks. The nodes job in a traveling environment in which they are freely allowed to join as well as to leave the wireless network anytime. As any of the node comes within the network radio range it will automatically able to communicate with other nodes..
3) *Cooperativeness:* Usually assumes nodes are cooperative and non-malicious assumed by various Routing algorithms in MANETs. This results a malicious attacker easily turn into routing agent and disrupt network operation.
4) *Limited power supply*: Several problems formed due the restricted power supply in mobile ad-hoc networks and also power supply be considered as limited in MANETs. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.
5) *Adversary inside the Network*: In MANETs mobile nodes are free to join also to leave the network anytime. Network nodes also behave malicious in network range. There is no way to detect whether the node behavior is malicious or not. Hence internal attacks are more dangerous than external attacks.

3. Security Goals

All networking functions in MANETs like routing packets as well as forwarding are self organized and performed by nodes themselves. Therefore providing security to mobile ad -hoc networks is challenging task. To evaluate whether mobile ad-hoc networks are secure or not, so various goals must satisfied like as follows [3]:

1) *Availability:* At suitable times assets are available or accessible by authorized users is known as availability. Both of data and services come under availability. All network services should be always available even though denial of service attacks occurs.
2) *Confidentiality*: Confidentiality guarantees about all assets of computer are available only for authorized parties and accessed only by them. Information exchanged between participants should be protected from un-authorized users in MANETs. Eavesdropping and unauthorized access to message the two disclosure attacks should be protected.
3) *Integrity*: Integrity provides a way to access the assets in such a way that only the authorized users can access or modify the information. Information should be original while transferred to the user to ensure Integrity.
4) *Authentication:* Authentication means that the participants within the network communication are all authorized not fake. The assets of MANETs should be accessed only by authenticated nodes.
5) *Authorization*: Authorization means assigning various access rights like read, write and both to variant types of participants or users. Let's take an example of network admin that only assigned to perform network management tasks.
6) *Flexible to attacks:* The network functionalities of various types should be maintained if a no of nodes are lost or compromised.
7) *Originality:* Originality means newness that ensures about the previously snatched packets does not retransmitted by the malicious node.

4. Routing Protocols

Mobile Ad-Hoc network routing protocols [5,13,11] mainly divided into three classes: *Proactive*, *reactive* and *hybrid* protocols as shown in figure 2.

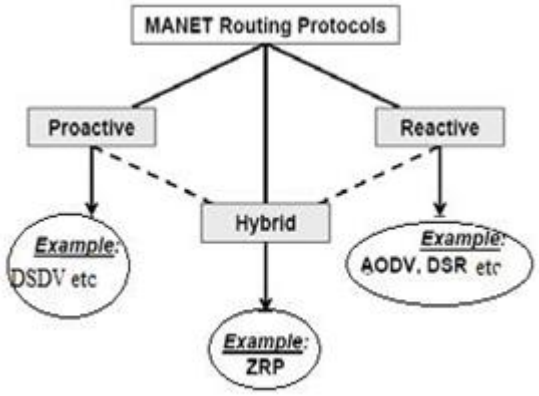

Figure 2: Classification of MANETs routing protocols

1) *Proactive Protocols***:** Proactive are also called as table-driven routing protocols of MANETs. In table driven routing, one or more tables are maintained for each node for store routing information and also any changes done within network necessarily being reflect by processing regular updates throughout the whole network for maintaining a consistency in viewing network. Conventional routing schemes are such schemes as an example: Destination sequenced distance vector routing protocol. Whole network information is maintained consistent and up-to-date. This allows nodes to quickly reestablish the network connections and minimizes the delay in communication. It also be determined which node is reachable or present in the network[1,8]

2) *Reactive Protocols:* Reactive are also called as on-demand routing protocol because of their behavior of not maintaining the routing information and also the routing activity in the network if no communication found between the nodes. Any node wants to send a data packet to another then searching is done on on-demand basis. After search route establishment is done for transmitting and receiving packets. The route request packets are flooded throughout the network for route discovery. Reactive routing protocols Examples are: (AODV) Ad-hoc on-demand Distance Vector routing and Dynamic Source Routing (DSR) [9].
3) *Hybrid Protocols:* Hybrid protocols[12] model is combination of reactive and proactive routing protocols. Example of hybrid routing protocols is ZRP. In Zone Routing Protocol (ZRP) whole network is divided into zones. It means ZRP exhibit hierarchical architecture in which each and every node maintains additional information related to topology of network by extra memory.

5. Classification of security Attacks

On the basis of behavior attacks be categorized as Passive or Active attack [2, 7]

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.
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. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than 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 classified into four groups:

   i. *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.
   ii. *Modification Attacks:*. These attacks modify packets and disrupt the overall communication between network nodes. Sinkhole attacks are the example of modification attacks.
   iii. *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.

A. Attacks at Physical Layer

Some of the attacks identified at physical layer include eavesdropping, interference, and jamming etc.

1) *Eavesdropping:* It can also be defined as interception and reading of messages and conversations by unintended receivers. The main aim of such attacks is to obtain the confidential information that should be kept secret during the communication.
2) *Jamming:* Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. Jamming attacks also prevents the reception of legitimate packets.
3) *Active Interference:* An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications.

B. Attacks at Data link layer

The data link layer can classify attacks as to what effect it has on the state of the network as a whole.

1) *Selfish Misbehaviour of Nodes:* The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources and to conserve of battery power.
2) *Malicious Behaviour of nodes* The main task of malicious node is to disrupt normal operation of routing protocol. The impact of such attack is increased when the communication takes place between neighboring nodes. Attacks of such type are fall into following categories.
3) *Denial of Service (DoS):* The prevention of authorized access to resources or the delaying of time-critical operations. A denial of service (DoS) attack is characterized by an attempt by an attacker to prevent legitimate users of a service from using the desired resources and attempts to "flood" a network, thereby preventing legitimate network traffic.
4) *Misdirecting traffic***:** A malicious node advertises wrong routing information in order to get secure data before the actual route.
5) *Attacking neighbor sensing protocols***:** malicious nodes advertise fake error messages so that important links interface are marked as broken.

C. Attacks at Network Layer

The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic.

1) Blackhole Attack: In this type of attacks[3,4], 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 to originator node .whose RREQ packets it wants to intercept. For example, in figure 3, When node "S" wants to send data to destination node "D", it initiates the route discovery process. The malicious node "M" when receives the route request, it immediately sends response to source. If reply from node "M" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node "M". As a result, all data packets are consumed or lost at malicious node.

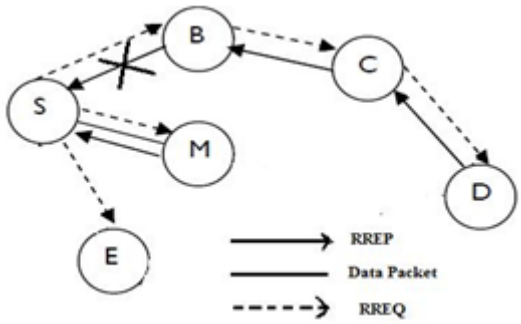

Figure 3: Blackhole Attack

2) Rushing Attack: In rushing attacks when compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet For example, in figure 4 the node "4" represents the rushing attack node, where "S" and "D" refers to source and destination nodes. The rushing attack of compromised node "4" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than those from other nodes. This result in when neighboring node of "D" i.e. "7" and "8" when receive the actual (late) route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any useable route or safe route without the involvement of attacker.

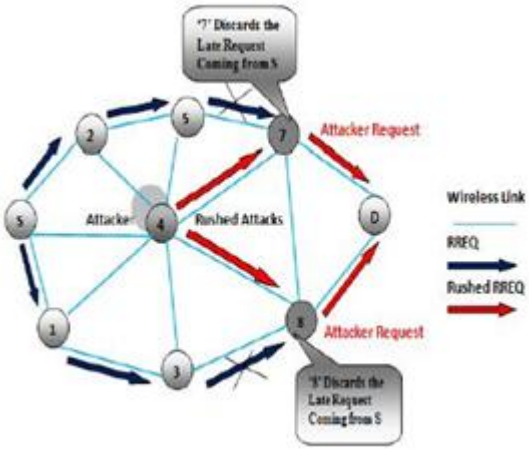

Figure 4: Rushing Attack

3) *Wormhole Attack*: The wormhole attack is one of the most efficient and merciless attacks, which can be executed within MANETs. Therefore two collaborating attackers should establish the so called wormhole link (using private high speed network e.g. over Ethernet cable or optical link): connection via a direct low-latency communication link between two separated distant points within MANETs. As soon as this direct bridge (wormhole link) is built up one of the attackers captures data exchange packets, sends them via the wormhole link to the second one and he replays them.

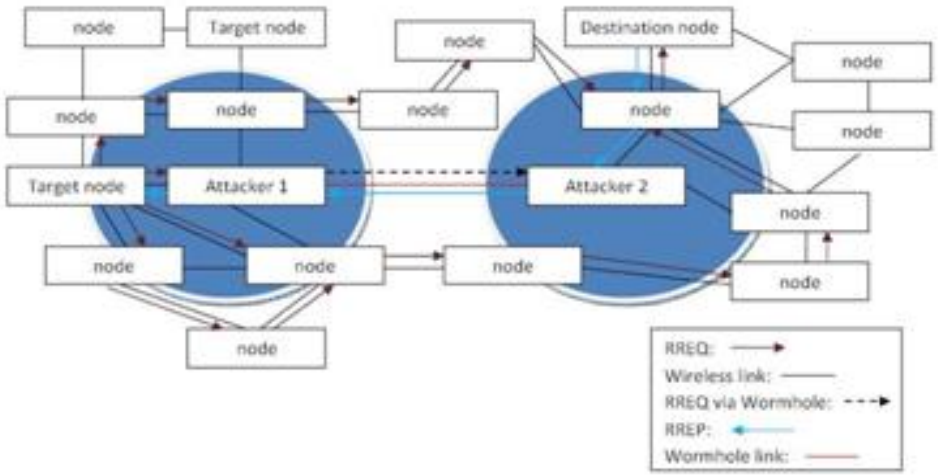

Figure 5: Wormhole Attack

4) Greyhole attack: In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. It is similar to blackhole attack but it drops data packet of a particular node.

5) 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.

D. Attacks at Transport Layer

1) 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 attacks.

E. Attacks at Application Layer

1) Malicious code attacks: Malicious code attacks include, Viruses, Worms can attack both operating system and user application.

6. Conclusion

MANETs are highly vulnerable to so many attacks because of dynamic topology used in MANETs, its distributed operations and also of limited bandwidth. In this review paper, we have discussed about MANETs and its few characteristics, advantages challenges, some of its applications, security goals, types of security attacks in MANETs routing protocols. These security attacks further classified into active attacks and passive attacks. Futuristic view of ad- hoc networks is very charming, giving a high vision of focus on anytime, anywhere and also cheap communications.

Before these imagined scenarios come true, a very large amount of work done in both researching process and implementation. At the present state, the common trends in MANETs are towards mesh architecture and large scale architectures. Improvement in MANETs both bandwidth and capacity is highly required, which implies the need for a higher frequency and better spatial spectral reuse.

References

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

[2] Mohammad Wazid**,** Rajesh Kumar Singh and R. H. Goudar, *"A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques* **"** International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011.

[3] Aarti, *"Study of MANET: Characteristics, Challenges, Application and Security Attacks"*, IJARCSSE, Volume 3, Issue 5, pp. 252-257,May – 2013.

[4] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " *A survey of black hole attacks in wireless mobile ad hoc networks"* Human-centric Computing and Information Sciences 2011

[5] Sunil Taneja and Ashwani Kush, "A *Survey of Routing Protocols in Mobile Ad-Hoc Networks*", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, 279-285, August 2010.

[6] Gary Breed Editorial Director, "*Wireless Ad-Hoc Networks: Basic Concepts*", High Frequency Electronics,March 2007.

[7] Hongmei Deng, Wei Li, and Dharma P. Agrawal, *"Routing Security in Wireless Ad Hoc Networks"* IEEE Communications Magazine ,October 2002

[8] Mohseni, S.; Hassan, R.; Patel, A.; Razali, R, *"Comparative review study of reactive and proactive routing protocols in MANETs"*, 4th IEEE International Conference on Digital Ecosystems and Technologies, pp.304-309, April2010.

[9] Humayun Bakht, "*Survey of Routing Protocols for Mobile Ad-hoc Network*", International Journal of

Information and Communication Technology Research, pp.258-270, October 2011.

[10] Mohit Kumar and Rashmi Mishra "*An Overview of MANET: History, Challenges and Applications*", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 Issue 1, Mar 2012.

[11] Perkins, E. Belding-Royer and S. Das, "*Ad-Hoc On-Demand Distance Vector (AODV) Routing*", RFC3561, July 003.

[12] Murthy, S., Garcia-Luna-Aceves, J. J., "*An Efficient Routing Protocol for Wireless Networks*", MONET, Vol 1, No 2, pp. 183-197, October1996.

[13] Sampo Naski, "*performance of Ad Hoc Routing Protocols: Characteristics and Comparison*", Seminar on Internetworking, 2004.