Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study of MANET: Characteristics, Challenges, Application and Security Attacks

Aarti
Department of Computer Science & Engineering , MRIU Faridabad, Haryana, India.

Dr. S. S. Tyagi
Professor and Head, Department of computer science & Engineering, MRIU, Faridabad, India.

Abstract - Mobile ad hoc networks (MANETs) is an infrastructure-less , dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks like worm hole, black hole, rushing attack etc. In this paper we study mobile ad-hoc network and its characteristics, challenges, application, security goals and different types security attacks at different layers.

Keywords: Mobile ad-hoc network(MANET), Destination sequenced distance vector (DSDV), Ad-hoc On-demand Distance Vector routing (AODV), Dynamic Source Routing (DSR).

I. INTRODUCTION

A Mobile Adhoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others needs the aid of intermediate nodes to route their packets. Each of the node has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other, however the node 2 can be used to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

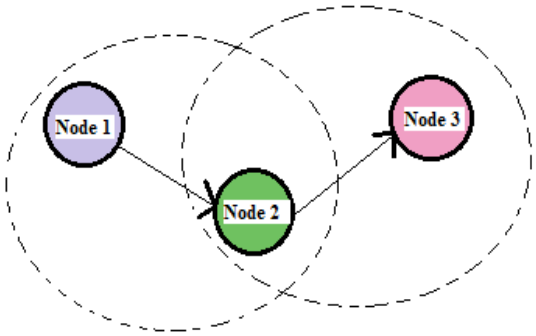

Fig. 1 Example of mobile ad-hoc network

A. MANETs characteristics

1) Distributed operation: There is no background network for the central control of the network operations, the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

2) Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3) Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

4) Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing 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.

B. Advantages of MANET

The advantages of an Ad-Hoc network include the following:

- They provide access to information and services regardless of geographic position.
- Independence from central network administration. Self-configuring network, nodes are also act as routers. Less expensive as compared to wired network.
- Scalable—accommodates the addition of more nodes.
- Improved Flexiblibility.
- Robust due to decentralize administration.
- The network can be set up at any place and time.

C. MANETs Challenges

1) Limited bandwidth: Wireless link continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communication after accounting for the effect of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

2) Dynamic topology: Dynamic topology membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

3) Routing Overhead: In wireless adhoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

*4) Hidden terminal problem***:** The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

5) Packet losses due to transmission errors: Ad hoc wireless networks experiences a much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni-directional links, frequent path breaks due to mobility of nodes.

6) Mobility-induced route changes: The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

7) Battery constraints: Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

8) Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

D. MANETs Applications

Some of the typical applications include:

1)Military battlefield: 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 head quarter.

2) Collaborative work: For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

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

4) Personal area network and bluetooth : A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

5) 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.

II. MANET VULNERABILIES

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[1]. 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.

2) 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. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node.

3) 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.

4) 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.

5) Adversary inside the Network: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack.

III. SECURITY GOALS

In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. 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.

2) Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. Protection of information which is exchanging through a MANET. It should be protected against any disclosure attack like eavesdropping- unauthorized reading of message.

3) Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way.. Integrity assures that a message being transferred is never corrupted.

4) Authentication: Authentication is essentially assurance that participants in communication are authenticated and not impersonators. The recourses of network should be accessed by the authenticated nodes.

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

6) Resilience to attacks: It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

7) Freshness: It ensures that malicious node does not resend previously captured packets.

IV. ROUTING PROTOCOLS

Ad-Hoc network routing protocols are commonly divided into three main classes; *Proactive* , *reactive* and *hybrid* protocols as shown in figure 2.

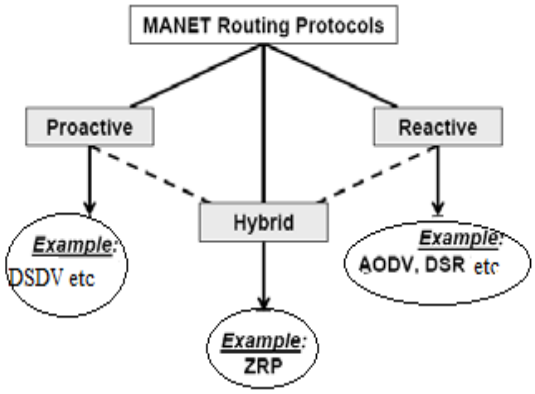

Fig. 2 Classification of MANET routing protocols

*1) Proactive Protocols***:** Proactive, or table-driven routing protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. Example of such schemes are the conventional routing schemes: Destination sequenced distance vector (DSDV). They attempt to maintain consistent, up-to-date routing information of the whole network. It minimizes the delay in communication and allow nodes to quickly determine which nodes are present or reachable in the network.

2) Reactive Protocols: Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV)[11] and Dynamic Source Routing (DSR).

3) Hybrid Protocols: They introduces a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extra memory.

V. Classification of security Attacks

The attacks can be categorized on the basis of behavior of the attack i.e. Passive or Active attack[2].

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 unauthorised 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:
1) 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.
2) Modification Attacks:. These attacks modify packets and disrupt the overall communication between network nodes. Sinkhole attacks are the example of modification attacks.
3) Fabrication Attacks: In fabrication attack, the attacker send fake message to the neighbouring 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 classified 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 neighbouring 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 neighbour 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, 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.

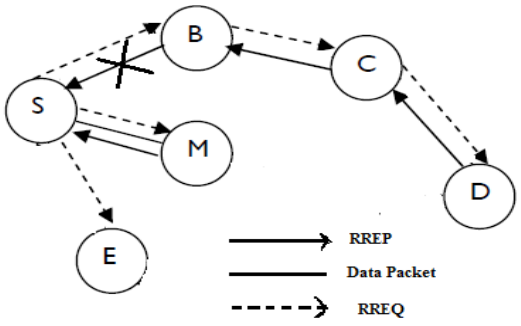

Fig. 3 Blackhole Attack

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.

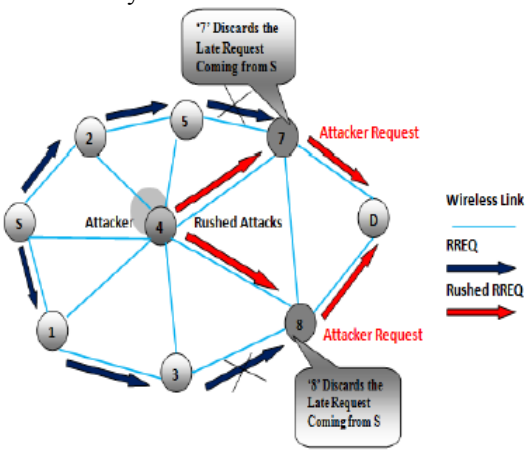

Fig. 4 Rushing Attack

3) *Wormhole Attack*: In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. For example in figure 5, the nodes "X" and "Y" are malicious node that forms the tunnel in network. The Originating node "S" when initiate the RREQ message to find the route to node "D" destination node. The immediate neighbor node of Originating node "S", namely "A" and "C" forwards the RREQ message to their respective neighbours "H" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbour node "B", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-A-B-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus, invalidates the legitimate route <S-C-H-E-F-D>.

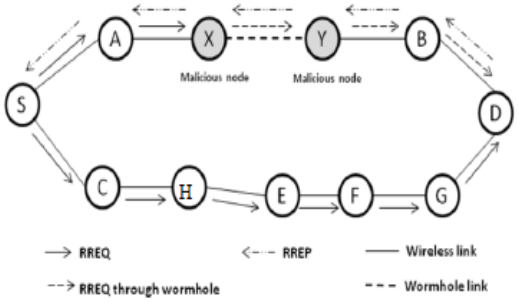

Fig. 5 Wormhole Attack

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.

VI. CONCLUSION

Due to dynamic topology, distributed operation and limited bandwidth MANET is more vulnerable to many attacks. In this paper, we discuss MANET and its characteristics, challenges, advantages, application, security goals, various types of security attacks in its routing protocols. Security attack can classified as a active or passive attacks . Different security mechanisms are introduced in order to prevent such network.

REFERENCES

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

[2]. Gagandeep, Aashima and Pawan Kumar "*Analysis of Different Security Attacks in MANETs on Protocol Stack*". International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012

[3]. 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.

[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, 304-309, 2010.

[9] Humayun Bakht, " *Survey of Routing Protocols for Mobile Ad-hoc Network*", International Journal of Information and Communication Technology Research, 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 No. 1 Feb-Mar 2012.

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

Aarti has done M.Tech. in Computer Engineering from Manav Rachna International University and B.TECH degree in Computer Science and Engineering with Distinction from Punjab Technical University. Her areas of interests are Networking, Security Mechanism

Dr. S. S. Tyagi is a Proferssor and Head at the Department of Computer Science and Engineering in Manav Rachna International University, Faridabad. He did his Ph.D from Kurukshetra University and has published many Papers in National and International journals and guiding Ph.D Scholars in the fields of Computer science and Engg.

