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 On MANET:An Overview

Swati Saini[*]
SES,BPS UNIVERSITY,
KHANPUR KALAN, SONIPAT
India.

Vinod Saroha
SES,BPS UNIVERSITY,
KHANPUR KALAN ,SONIPAT
India.

Abstract— As the increase of wireless networks, use of mobile phones, smart devices are gaining popularity so the adhoc network is also an uprising field. Each device in a MANET is free to move independently in any direction, linking to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. Its routing protocol has to be able to cope with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply etc. This paper describes the features, application, and vulnerabilities of mobile ad hoc network also presents an overview and the study of the attacks.

Keywords— MANET, Wireless Networks, Ad hoc Networking, Routing Protocol

I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism

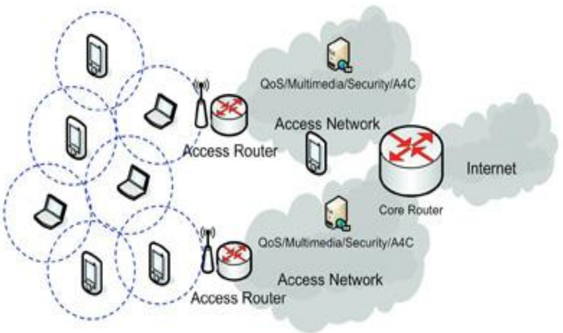


Figure 1:.Mobile Adhoc Network

II. CHARACTERISTICS OF MANET

MANETs have several salient characteristics:

A. Dynamic topologies:

Nodes are free to move arbitrarily; thus, the network topology--which is typically multi-hop may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

B. Bandwidth-constrained, variable capacity links

Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions,etc.--is often much less than a radio's maximum transmission rate.

C. Energy-constrained operation

Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.

D. Limited physical security

Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet

III. APPLICATIONS OF MANET

A. Defence

- Military communication and operations
- Automated battlefields

B. Emergency services

- Search and rescue operations
- Disaster recovery
- Replacement of fixed infrastructure in case of environment
- Policing and fire fighting
- Supporting doctors and nurses in hospitals

C. Education

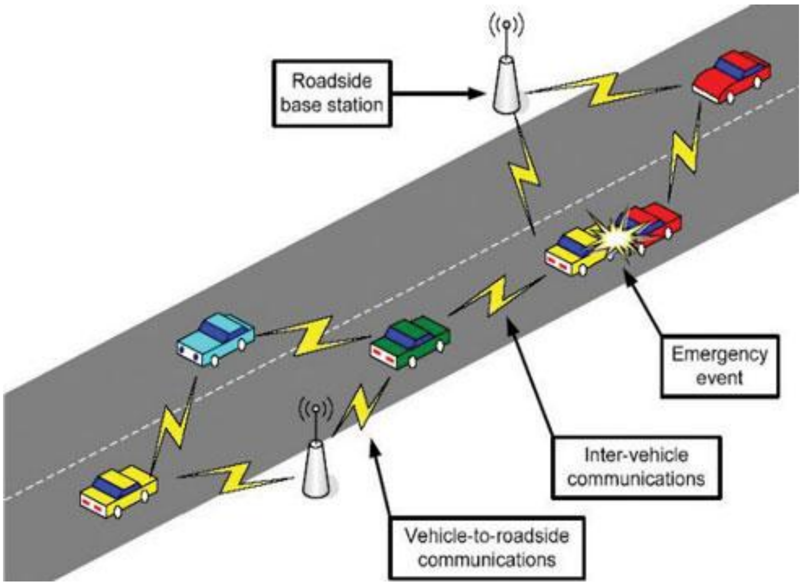
- Universities and campus settings
- Virtual classrooms
- Ad hoc communications during meetings or lectures

D. Entertainment

- Multi-user games
- Wireless P2P networking

IV.TYPES OF MANET

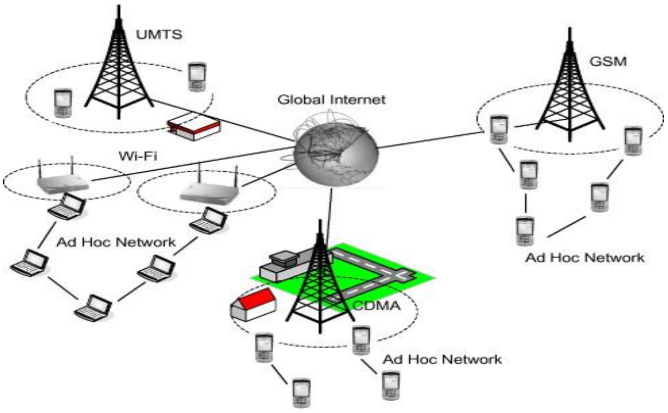
Vehicular Ad Hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment. VANET is a special class of Mobile Adhoc Networks (MANET), in which the nodes are the vehicles which communicate with other vehicles or with the base station which acts as a roadside infrastructure for using security and services application


Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Vehicular adhoc network(VANETS)

Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

Internet Based Mobile Ad-hoc Networks (iMANET) are ad-hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad-hoc routing algorithms don't apply directly.



Internet Based Mobile Ad-hoc Networks (iMANET

V. SECURITY GOALS

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.

Confidentiality:

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

Integrity:

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

Authentication:

Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured.

VI. CLASSIFICATION OF ATTACKS IN MANET

A. External and Internal Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

B.Active and Passive Attack

When the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network .Active attacks can an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network . In Passive attack, the attacker listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

VII. DIFFERENT ATTACKS IN MANET

A.Wormhole attack: A malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel**.**

B. Blackhole attack: In a black hole attack a malicious node advertising itself as having a valid route to the destination. With this intension the attacker consume or intercept the packet without any forwarding . An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped.

C. Byzantine attack: A compromised with set of intermediate, or intermediate nodes that working alone within the network carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services within the network

D. Rushing attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack . The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocol.
E.Replay attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions

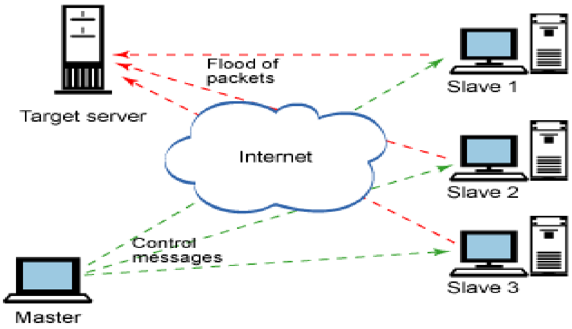
F. Location disclosure attack: An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques or with simpler probing and monitoring approaches Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.

G.Jellyfish attack: Similar to the blackhole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and delay jitter, and thus degrades the performance of real-time applications.

VIII. ATTACKS COMPARED

Denial of Service

In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network. A denial of service (DoS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the network protocol stack [13]. On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routingprotocol to disrupt the normal functioning of the network

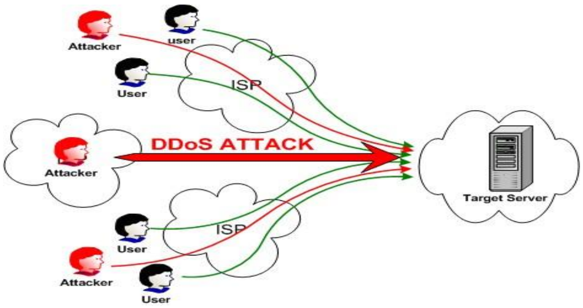


Denial of service attack

Some of the DoS attacks are described below:
Jamming: In this form of attack, the attacker initially keeps monitoring the wireless medium in order to determine the frequency at which the destination node is receiving signals from the sender. It then transmits signals on that frequency so that error-free reception at the receiver is hindered. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques.
SYN Flooding: In this form of attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN-ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the response of ACK packet. Without any response of ACK packets, the half-open data structure remains in the victim node. If the victim node stores these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node would not be able to accept any other legitimate attempts to open a connection. Normally there is a time-out associated with a pending connection, so the half-open connections will

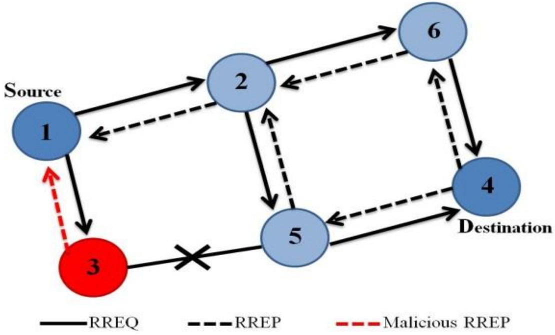
eventually expire and the victim node will recover. However, malicious nodes can simply continue sending packets that request new connections faster than the expiration of pending connections.

Distributed DoS Attack: Distributed denial of service attack is more severe form of denial of service attack because in this attack several adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.



Distributed denial of service attack

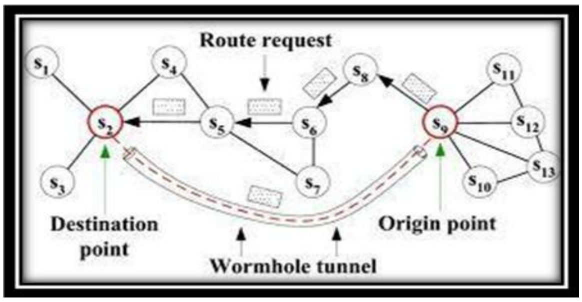
Blackhole attack: In a black hole attack a malicious node advertising itself as having a valid route to the destination. With this intension the attacker consume or intercept the packet without any forwarding An attacker can completely modify the packet and generate fake information, this cause the network traffic diverted or dropped.



Blackhole Attack

The single black hole black hole attack in the mobile ad hoc networks .Node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 1. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets problem.

Wormhole attack: Tunneling attack is also called wormhole attack. In a tunnelling attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. It is called tunneling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers



Warmhole attack

References

[1] L. Buttyan and J. Hubaux, “Stimulating cooperation in selforganizing mobile ad hoc networks,” ACM/Kluwer MobileNetworks and Applications (MONET) 8 (2003).

[2] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V.Vijayaraghavan, “Participation incentives for ad hocnetworks,” http://www.stanford.edu/~yl31/adhoc (2001).

[3] D. Barreto, Y. Liu, J. Pan and F. Wang, “Reputation-basedparticipation enforcement for adhoc networks,”http://www.stanford.edu/~yl314/adhoc (2002).

[4] Y.C. Hu, A. Perrig, and D.B. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”, Proceedings of ACM WiSe 2003, San Diego, CA, Sep. 2003.

[5] E.M. Royer and C.E. Perkins, “Multicast Operation of the Ad Hoc On-Demand Distance Vector Routing Protocol”, Proceed- ings of MobiCom ’99, Seattle, WA, Aug. 1999, pp. 207-218.

[6] QualNet Simulator, http://www.qualnet.com

[7] J. G. Jetcheva and D.B. Johnson, “Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Net

[8] M.S. Corson, J.P. Maker and J.H. Cernicione, Internet- based Mobile Ad hoc Networking, IEEE Internet Computing, pages 63- 70, July- August 1999.

[9] A Mishra and K.M Nadkarni, security in wireless Ad hoc network, in Book. The Hand book of Ad Hoc Wireless Networks(chapter 30), CRC press LLC, 2003.

[10] Y. Haung and W. Lee, A Cooperative Intrusion Detection system for Ad hoc Networks, in Proceedings of the 1st ACM Workshop on security of Ad hoc and sensor Networks, Fairfax, Virgining 2003, pages 135-147.

[11] I. Aad, J.-P. Hubaux, and E. W. Knightly, “Denial of Service Resilience in Ad Hoc Networks,” in Proceedings of the 10th Annual International Conference on Mobile Computing and Networking. Philadelphia, PA, USA: ACM Press, Sep. 2004,

[12] Noyes, Katherine. "Which Linux Distro Is Fairest of Them All? Ubuntu, Survey Says". *PCWorld*. Retrieved 2012-07-08.

[13] Zachte, Eric. "Wikimedia Traffic Analysis Report - Operating Systems".*Wikimedia Traffic Analysis Report*. Wikimedia Foundation. Retrieved 2012-07-08.

[14] M. Al-Shurman, S.-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” in Proceedings of the 42nd Annual ACM Southeast Regional Conference. Huntsville, AL, USA: ACM Press, Apr. 2004, pp. 96–97.

[15] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” in Proceedings of the 6th Annual International Conference on Mobile computing and Networking. Boston, MA,