www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-4, Issue-2, Apr 2016
Review Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Introduction to MANET

P. Chouksey

Dept. of CSE, Technocrats Institute of Technology, RGT University, Bhopal, India

Received: Mar/14/2016 Revised: Mar/26/2016 Accepted: Apr/20/2016 Published: Apr/30/2016

Abstract— Mobile Ad Hoc Networks (MANETs) has become the mainly up-coming field of recent research areas. MANET is the novel rising technology in which communication can be done with no any physical communications regardless of their geographical place. This is the cause why MANET is from time to time referred to as "infrastructure less network". It's nature is self organized as well as adaptive. Connections between the devices are maintained in ad-hoc network. Adding up and removal of devices to and from the network are very simple, but due to nodal mobility, the network topology may vary rapidly and randomly over time. In a disperse surroundings where the topology fluctuate, the routing of message is a big trouble. It is a collection of independent mobile nodes. Communication is done between these nodes via radio waves. Some of the mobile nodes are in radio range these nodes can directly communicate, whereas others needs the aid of middle nodes so that they can route their packet. For maintaining communication among different nodes each of the node has a wireless boundary.

Keywords—Component, Formatting, Style, Styling, Insert (key words)

I. INTRODUCTION

MANET is entirely distributed, and can work at several places, where network association and message delivery must be executed by the nodes themselves. It does not need any fixed transportation as access points or base stations. Figure 1 shows a plain 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[4].

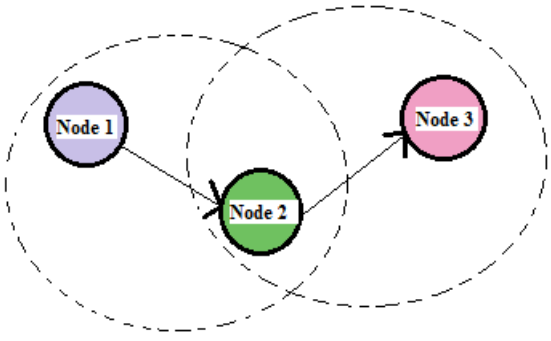

Figure 1. Example of mobile ad-hoc network

History of MANET

Ad-hoc networks are categorized into 3 types. Current ad-hoc networks systems are belongs to the third generation. The first generation goes back to 1972. The second generation of ad-hoc networks emerge in 1980s, and the ad-hoc network systems were improved and implemented as a part of the SURAN (Survivable Adaptive Radio Networks, commercial ad-hoc networks inwards with note-book computers and other viable communications equipment in) in 1990. At some research conferences the idea of a collection of mobile nodes was proposed. Since mid 1990s, a lot of work has been done on the ad hoc standards. Right now, there are two kinds of mobile wireless networks are existing. The first is infrastructure networks with fixed and wired gateways. Applications of this wireless network include wireless local area networks (WLANs). The second type of mobile wireless network is the infrastructure less mobile network, usually known as the MANET.

Types of MANET

Mobile ad-hoc network (MANET) is an ad-hoc network but an ad-hoc network is not essentially a MANET. On the basis of different use and the definition of MANET it can be of following types.

- Vehicular ad-hoc network (VANETs) – They are used for communication amongst vehicles and between vehicles.
- Internet based mobile ad hoc networks (iMANETs) - They are ad hoc networks and is use to connection mobile nodes and permanent Internet-gateway nodes.
- Military / Tatical MANETs - They are used

© 2016, IJSRNSC All Rights Reserved

by military units with stress on security, range, and integration with presented systems.

Characteristics of MANET

- MANET is autonomous in behaviour in which each node act as host as well as router.
- It is Multi-hop radio relaying i.e When a source and destination for a message is out of the radio range, then the MANETs can perform multi-hop routing.
- The nature of MANET is Distributed .A centralized firewall is absent in MANET.
- The nodes can join or leave the network very easily at anytime, it makes the network topology dynamic that changes with time.
- In MANET mobile nodes are available with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are the features. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behaviour of a MANET demands minimum human intervention to configure the network.
- All nodes have identical features and share similar responsibilities, capabilities which form symmetric environment.
- Nodal connectivity is intermittent.

MANET Vulnerabilities

Vulnerability is one of the weakness in security system. The confirmation of users individuality is an important step in the system. A particular system may be susceptible to unofficial data manipulation. MANET is more vulnerable than wired network. Following are the vulnerabilities are as follows:-

Lack of centralized management: One of the main problem of MANET is that it doesn't have a central monitor server which make the discovery of attacks hard because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network.

Resource availability: Resource availability is other main issue in MANET. It is not easy to provide secure communication in MANET where maintaining protection against threats and attacks are again very important. It lead to growth of a variety of security scheme and architectures. Ad-hoc environment also permit achievement of self-organized security mechanism.

- **Scalability**: The scale of ad-hoc network altering all the time due to mobility of nodes, So scalability is a major issue about safety. It is essential that safety mechanism should be able of handling a large network as well as small ones.
- **Cooperativeness**: Routing algorithm for MANETs usually assume that nodes are supportive and non-malicious. Malicious attacker can easily become an important routing agent.
- **Dynamic topology**: The network topology may alter fast and randomly over time due to nodal mobility, which is active in nature. Dynamic topology and variable nodes membership may upset the trust association among nodes. This dynamic behavior could be improved protected with distributed and adaptive security mechanisms.
- **No predefined Boundary**: In mobile ad-hoc networks it is impossible to define a physical limit of the network. The nodes can join and go away the wireless network at any time. As soon as an opponent comes in the radio range of a node it will be able to communicate with that node.
- **Bandwidth constraint:** As compare to wireless network **v**ariable low ability links exists which are more vulnerable to external noise, interference and signal attenuation effects.
- **Adversary inside the Network**: The nodes within network may also act maliciously. The mobile nodes within the MANET can freely join and leave the network, and this is one of the reason why it is not easy to detect the behavior of the node is malicious. These nodes are called compromise nodes.
- **Limited power supply**: The nodes in mobile ad-hoc network need to consider limited power supply, which will cause several problems.

Security Goals

All networking function such as routing and packet forwarding, are perform by nodes in MANET in a self-organizing manner. For these reasons, secure a mobile ad -hoc network is very challenging. Mobile ad-hoc network is secure or not it can be evaluate as follows:

- **Availability**: In ease of use authorized parties are accessible at suitable times. It ensures the survivability of network service in spite of denial of service attack.

© 2016, IJSRNSC All Rights Reserved

Availability apply both to data and to services.

- **Confidentiality**: Only those who should have access to something will actually get that access. We need to keep surreptitious all information from all entities that do not have licence to access them to preserve confidentiality of some confidential information. It is from time to time called secrecy or privacy.
- **Integrity**: In integrity asset can be modified only by authorized parties only in official way. Modification includes writing, changing status, deleting and creating. Integrity assure that the messages being transferred from the source is never corrupted.
- **Authentication**: Authentication enable a node to ensure the individuality of peer node it is communicating with. Authentication is the one in which it assure that participant in communication are genuine and not fake. In this authenticity is ensured because only the genuine sender can produce a message that will decrypt properly with the shared key.
- **Anonymity**: Anonymity can be given as that all information that can be used to identify current user of node should failure to pay be kept private and not be distributed by node itself or any other the system software.
- **Authorization**: This property assign different access privileges to different types of users. Such as a network management can be done by network manager only.

Broadcasting Approaches In MANET:

In MANET [5], a number of broadcasting approach on the basis of cardinality of destination set:

- Uni-casting: Sending a message from a source to a single purpose.
- Multicasting: Sending a message from a source to a set of destinations.
- Broadcasting: Flooding of messages from a source to all other nodes in the specified network.
- Geocasting: Sending a message from a source to all nodes inside a geographical region.

Attacks in MANET:

Securing wireless ad-hoc networks is a extremely challenging issue. The first step towards just beginning good security solution is to understanding all likely form of attacks possible in MANET. For secure transmission of information from side to side nodes communication security is important. In the absence of any security device and shared wireless medium MANET more vulnerable to digital and cyber attacks than wired network. There are a number of attacks that can affect MANET in many ways. These attacks can be classified into two types:

External Attack: External attacks are done by nodes that do not belong to the real network. It increase jamming in the network and sends fake routing information or causes unavailability of services.

Internal Attack: Internal attacks are done by those compromise nodes that are part of the network. In an internal attack the hateful node from the network gains unauthorized access and impersonate as a genuine node. This type of attack can analyze traffic between former nodes in the network and may contribute in other network activities.

On the basis of above categories following attacks are possible:

Denial of Service attack: DoS attack points to the availability of a node or the whole network. After DoS attack the services will not be available at any point. For this attack the attacker usually uses radio signal jamming and the battery exhaustion method.

Impersonation: In this attack in the absence of proper authentication or if the authentication mechanism is not correctly implement then the hateful node can act as a genuine node and frequently monitor the network traffic. It can also send fake routing packets, and gain access to some secret information using this attack.

Eavesdropping: This is a passive attack. Here the node without a sound observes the secret information, and these information can be afterwards used by the malicious node. Later the secret information such as location password, public key, private key, etc. can be fetch by eavesdropper.

Routing Attacks: The malicious node make routing services a aim because it is one of the significant service in MANETs. There are two types of routing attack. The first is on routing protocol and second is on packet forwarding or delivery mechanism. The first is carried at blocking the propagation of routing information to a node. The second is aimed at disturbing the packet delivery against a predefined path of the packet.

Black hole Attack: In this attack, an attacker sends a zero metric for all destinations which causes all nodes around it to route packets towards it.[6] A malicious node sends fake

© 2016, IJSRNSC All Rights Reserved

routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. After receiving all packets the malicious node drop all receiving packets instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol [4].

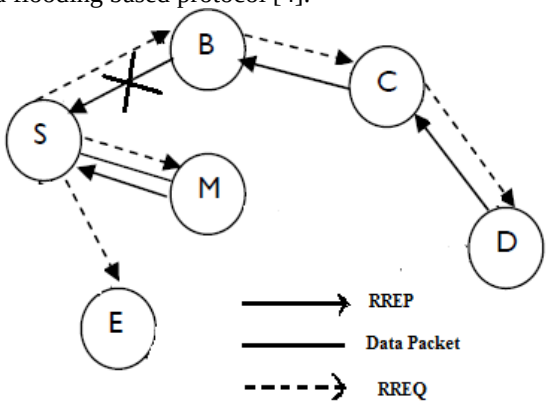

Figure 2. Blackhole Attack

Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network which are called tunnels and then send them to one more point in the network, and send replays them into the network from that point. When routing control message are tunnel at that point routing can be disrupt. This tunnel between two colluding attacks is known as a wormhole.

Replay Attack: In this attack attacker performs a replay attack and retransmitted the valid sent data repeatedly to increase the network routing traffic that has been capture before. This attack is done usually on new routes, but can also be used to weaken poorly designed security solutions.

Jamming: In jamming, initial attacker try to find at which frequency destination node is receiving signal from sender. Initially it keeps monitor wireless medium and then broadcast signal on that frequency so that error free receptor is caught up.

Man- in- the- middle attack: An attacker keep eye on sender and receiver and the data being sent between two nodes. In some of the cases, attacker can mimic the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Gray-hole attack: This attack is accountable for dropping of messages and also known as routing mis-behaviour attack. Gray hole attack has two phases. In the first phase the node promote itself as having a suitable route to destination where as in the second phase, nodes drops intercepted packet with a sure probability.

MANET Challenges:

The features of MANET have several challenges. These include :

Routing*:* As discussed above we know that the topology of the network is continually altering, so the issue of routing packets between any pair of nodes is a demanding task. Most protocols are based on reactive routing rather then practical. Multi cast routing is another problem because the multi cast tree is no longer static and the reason is the random movement of nodes within the network. Multiple hops are available between nodes in the route, which is more compound than the single hop communication.

Security and Reliability*:* In addition to the common vulnerabilities of wireless connection, an ad hoc network has security issue due to mean neighbour relaying packets. Distributed operation needs different schemes of authentication with key management. Further, wireless link features introduce also reliability problems. The wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors take place due to limited broadcast range.

Quality of Service (QoS*):* It is a big challenge to provide dissimilar excellence of service in a continually changing environment . An adaptive QoS is used in implementing over the traditional resource condition to support the multimedia services.

Inter-networking: The communication within an ad hoc network, inter-networking between MANET and fixed networks (in IP based) is usually expected in so many cases. The coexistence of routing protocols in these mobile device is a confront specially for the tuneful mobility management.

Power Consumption: The communication-related functions should be optimized for lean power consumption specially in light-weight mobile terminals. Conservation of power and power-aware routing must be taken into consideration.

Multicast: Multicast is attractive to hold up multiparty wireless communications. Since the multicast tree is no longer static, therefore the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join).

Location-aided Routing: It is used to position information which is used to define linked regions so that the routing is spatially oriented and limited.

© 2016, IJSRNSC All Rights Reserved

References

[1] Himadri Nath Saha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee ,Aniruddha Bhattacharyya ,Arnab Banerjee , Dipayan Bose "*Study Of Different Attacks In Manet With Its Detection & Mitigation Schemes*" International Journal of Advanced Engineering Technology IJAET/Vol.III/ Issue I/January-March, 2012/383-388.

[2] Yu-seung Kim, Heejo Lee., "*On classifying and evaluating the effect of jamming attack.*"

[3] Ali Hamieh, Jalel Ben-Othman. "*Detection of jamming attacks in wireless ad hoc networks using errordistribution.*", p.p.1-6,IEEE 2009.

[4] Dr. S. S. Tyagi, "*Study of MANET: Characteristics, Challenges, Application and Security Attacks*", Volume 3, Issue 5, May 2013

[5] IIyas, M., "*The hand book of ad -hoc wireless networks*", CRC press LLC. 2003

[6] Broch,J., A.M David and B. David,1998, "*A Performance comparison of multi-hop wireless ad hoc network routing protocols*", Proc.IEEE/ACM MOBICOM'98, pp: 85-97.

[7] M. Frodigh, P. Johansson, and P. Larsson., "*Wireless ad hoc networking: the art of networking without a network*," Ericsson Review,No.4, 2000, pp. 248-263.

[8] E. M. Royer and C-K Toh, "*A review of Current routing protocols for Ad Hoc Mobile Wireless*."

[9] Y. Hu, D. Johnson and A Perrig, "*SEAD: Secure Efficient Distance Vector Routing for Mobile Wire*."

[10] D. Johnson and D. Maltz, "*Dynamic Source Routing in Ad Hoc Wireless Network‖ Mobile Computing*", T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[11] Belding-Royer,E.M. and C.K. Toh, "*A review of current routing protocols for ad-hoc mobile wireless networks*." IEEE Personal Communication magazine pp:46-55. 1999

[12] M. Frodigh, P. Johansson, and P. Larsson., "*Wireless ad hoc networking: the art of networking without a network*," Ericsson Review,No.4, 2000, pp. 248-263.

[13] Snehita Modi, Dr. Paramjeet Singh, Dr. Shaveta Rani, "*Performance Improvement of Mobile Ad hoc Networks under Jamming Attack"* (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5197-5200

[14] M. Kumar, T. Singh, "*A Survey on Security Issue in Mobile AD-HOC Network and Solutions*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.71-75, 2014.

[15] Vinod Mahor, Sandeep Raghuwanshi, "*Loss Function Based Measurement of Mobile Ad-Hoc Network Parameters under AODV Routing Protocol*", IEEE – 31661 4th ICCCNT - 2013 July 4-6, 2013, Tiruchengode, India.

[16] Ali Hamieh, Jalel Ben-Othman. "*Detection of jamming attacks in wireless ad hoc networks using error distribution.*" p.p.1-6,IEEE 2009.

[17] Wenyuan Xu, Wade Trappe,Yanyong Zhang and Timothy Wood. *"The feasibility of launching and detectingjamming attacks in wireless networks."*

[18] John Dunlop and Joan Cortes. "*Impact of Directional Antennas in Wireless Sensor Networks.*", pp.1-6, IEEE 2007.

[19] Ali Hamieh, Jalel Ben-Othman. "*Detection of jamming attacks in wireless ad hoc networks using error distribution.*" p.p.1-6,IEEE 2009.

© 2016, IJSRNSC All Rights Reserved