Volume 8, No. 4, May 2017 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Vulnerabilities & Attacks in Mobile Adhoc Networks (MANET)

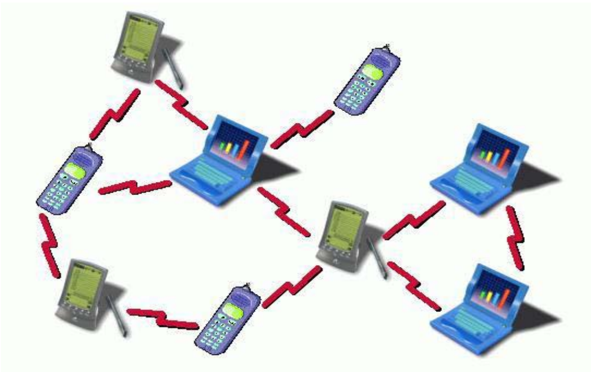
Dr. Gurjeet Singh Dhillon
Dean Academics
MK Group of Institutes
Amritsar, Punjab, India

***Abstract:* Mobile Ad-Hoc Network (MANET) is an infrastructure less wireless network of autonomous collection of mobile nodes. Network is self-configured to reconstruct its topology and routing table information for the exchange of data packets on the joining and leaving of each node on ad-hoc basis. This paper is based on the Vulnerabilities, Applications & Challenges in MANET.**

***Keywords*: MANET, MANET Challenges & Applications**

I. Introduction to Mobile Adhoc Networks

It is an infrastructure less IP based network of mobile and wireless machine nodes connected with radio. In operation, the nodes of a MANET do not have a centralized administration mechanism. It is known for its routable network properties where each node act as a “router” to forward the traffic to other specified node in the network.Many new applications are resulted from progress in the internet discipline because of wireless network technologies. For research and development of wireless network, one of the most auspicious arenas is Mobile Adhoc Network (MANET).



Figure

Wireless ad-hoc network is becoming one of the most animated and dynamic field of communication and networks because of fame of movable device and wireless networks that has increased significantly in recent years. A mobile ad-hoc network is formed by collecting portable devices like laptops, smart phones, sensors, etc. that communicate through wireless links with one another. These devices collaborate with each other to offer the essential network functions in the non appearance of immovable organization in a distributed manner. This type of network creates the way for various innovative and stimulating applications by functioning as an independent network or with multiple points of connection to cellular networks or the Internet. Routing of packets to destination is done by the cooperation of nodes of a MANET.

The sending and receiving devices may be situated at a much higher distance as compared to transmission radius R, however, each network node can communicate only with nodes placed within its broadcast radius R. All the nodes in a multihop wireless ad-hoc network collaborate with one another to create a network in the absence of infrastructure such as access point or base station.

In order to permit transmission among devices beyond the transmission range in MANET, the mobile devices require advancing data-packets for one another. The network devices can move freely and autonomously in any route. The nodes can detach and attach to the network haphazardly. Thus variations in link states of the node with other nodes are experienced by a node regularly. Challenges for routing protocols operating in MANET are eventually increased the movement in the ad-hoc network, changes in link states and other characteristics of wireless transmission such as attenuation, multipath propagation, interference etc. The challenges are boosted by the numerous sorts of nodes of restricted processing power and competences that may join the network.

II. Characteristics of MANET

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.

III. Manet 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.

IV. 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.

V. MANET VULNERABILITIES

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. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

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. Lack of centralized management will impede trust management for nodes.
Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.
Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.
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 by disobeying the protocol specifications.
Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.
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.
Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

VI. Attacks in MANET

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

Internal Attack: Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

Routing Attacks: The malicious node make routing services a target because it’s an important service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

Black hole Attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it.[9] A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

Wormhole Attack: In a wormhole 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. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

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.

Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered

Man- in- the- middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Gray-hole attack: This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

Conclusion

The future of ad- hoc networks is really appealing, giving the vision of anytime, anywhere and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. At present, the general trend in MANET is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in ad- hoc networks). Large scale ad hoc networks are another challenging issue in the near future which can be already foreseen. As the involvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all forms.

References

[1] E. Alotaibi and B. Mukherjee, “A survey on routing algorithms for wireless Ad -Hoc and mesh networks ,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 56, no. 2, pp. 940–965, October 2011.

[2] M. Zhang and P. H. J. Chong, “Performance Comparison of Flat and Cluster -Based Hierarchical Ad Hoc Routing with Entity and Group Mobility ,” in Proc. of IEEE Communications Society conference on Wireless Communications & Networking, Budapest, Hungary, 2009, pp. 2450-2455.

[3] D. Dharmaraju, M. Karir, J. S. Baras, and S. Bas, “An Implementation Study of Multicast Extensions of AODV,” in Proc. of International Symposium on Performance Evaluation of Computer and Telecommunication Systems, Montreal, Canada, July 20-24, 2003, pp. 122-130

[4] M. A. Jaafar and Z. A. Zukarnain, “Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment,” European Journal of Scientific Research, ISSN 1450-216X, vol. 32, no. 3, pp. 430-443, 2009.

[5] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Ed. Kluwer Academic Publishers, 1996, vol. 5, pp. 153-181.

[6] Natarajan Meghanathan, “Impact of the Gauss-Markov Mobility Model on Network Connectivity, Lifetime and Hop Count of Routes for Mobile Ad hoc Networks”, JOURNAL OF NETWORKS, VOL. 5, NO. 5, MAY 2010, Page No.509

[7] Yasser Kamal Hassan, Mohamed Hashim Abd El-Aziz, and Ahmed Safwat Abd El-Radi , “Performance Evaluation of Mobility Speed over MANET Routing Protocols”, International Journal of Network Security, Vol.11, No.3, PP.128{138, Nov. 2010, Page No.128