A Need for Security in MANET

Usha Rani J[1], Sowmya M[2]
[1, 2] Department of Computer Science
[1, 2] GSSSIETW, Mysuru

Abstract- *In todays networking world in order to provide protected communication between mobile nodes Security has become a primary concern and major step. manet is having its own distinict characteristics related to the security issues. The unique characteristics of networks of mobile pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, tringent resource constraints, and highly dynamic network topology... The complete security solution should encompass all three security components of prevention, detection, and reaction. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In this paper, we discuss security issues, vulnerable nature of the mobile ad hoc network, security criteria and the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network and then conclude this paper.*

Keywords- MANET, Advantages and Disadvantages, Security Attributes, Attacks

I. INTRODUCTION

Mobile adhoc networks (MANETs) have received tremendous attention in recent years because of their self-configuration and self-maintenance capabilities. A mobile adhoc network (MANET) is generally defined as a network that has many free or autonomous nodes, often composed of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without strict top-down network administration. It is wireless network where mobile hosts forms a temporary network without the aid of any centralized administration or standard support services[1].

Figure (1) Example of Manet Architecture

Example scenarios for MANETs Meetings, Emergency or disaster relief situations, Military communications Wearable computers, Sensor networks.

Features of MANET

- It Rapidly deployable, self configuring.
- No need for existing infrastructure.
- Wireless links.
- Nodes are mobile, topology can be very dynamic.
- Nodes must be able to relay traffic since communicating nodes might be out of range.
- A MANET can be a standalone network or it can be connected to external networks(Internet).
- Energy constrained operation
- Longer transmission range due to multi-hop relay
- It works in the manner of distributed operation

ADVANTAGES OF MANET

- **Rapid deployable-**The nodes in adhoc network need not rely on any hardware and software. So, it can be connected and communicated quickly. Self configurable in manet Self-configuring nodes are also routers so it can configure individually without any support and Self-healing is done through continuous re-configuration
- **Mobility-**allows mobile adhoc networks created on the fly in any situation where there are multiple wireless devices.
- **Does not require infrastructure to work** Flexible adhoc infrastructure can be temporarily setup at anytime, in any place so there is no need of any infrastructure.
- **It is cost effective-**Lower getting-started costs due to decentralized administration.
- **Less time consuming**
- **More robust than cellular system-** Manet is having an ability to provide temporary and instant wireless networking solutions in situations where cellular infrastructures are lacing and are expensive or infeasible to deploy due to this distributed nature Manetas are more robust than cellular counterparts against single-point failures.

DISADVANTAGES of MANET

- **Lack of centralized management**: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult. it cannot maintain traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

- **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**: 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.

- **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 compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.
- **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. These nodes are called compromised nodes.

- **No predefined Boundary**: In mobile adhoc 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 request comes in the radio range of a node it will be able to communicate with that node. The attacks include Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack

II. MANET CHALLENGES

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include

- **Routing:** Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

- **Security and Reliability:** In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility induced packet losses, and data transmission errors[3].

- **Quality of Service (QoS):** Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

- **Inter-networking:** In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

- **Power Consumption:** For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

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

- **Location-aided Routing:** Location-aided routing uses positioning information to define associated regions so that the routing is spatially oriented and limited. This is analogous to associatively-oriented and restricted broadcast in ABR.

III. MECHANISMS IN MANET

(i)Multihop operation ,(ii)routing mechanism designed for mobile nodes.(iii) Internet access mechanisms. (iv)Self configuring networks requires an address allocation mechanism. (v)Mechanism to detect and act on, merging of existing networks (vi)Security mechanisms.

IV. SECURITY ATTRIBUTES

Success in operations of a mobile adhoc network depends on cooperation of the nodes in providing services to each other. Since mobile adhoc networks make it possible for the devices to join or leave the domain without required permission, node in the domain can not considered to be trusted. Conventional security approaches do not address all concerns of ad hoc networks since both begin and malicious parties have full admission to communicate with peers. The wireless channel is accessible to both legitimate network users and malicious attackers. Attackers may intrude into the network through the subverted nodes. In spite of the dynamic nature, mobile users may apply for anytime, anywhere security services as they are in motion from one place to another[7]. Consequently a security solution is required which has both extensive protection and desirable network performance. Security involves a set of investments that are adequately funded. 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 adhoc network is very challenging.

Some of the attributes used to evaluate if mobile adhoc network is secure or not are as follows:

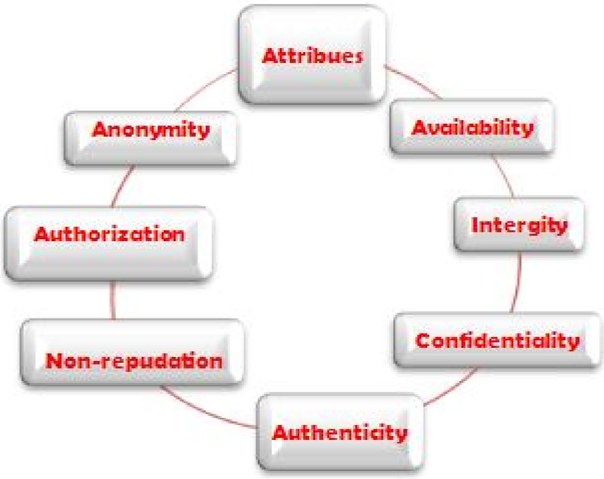


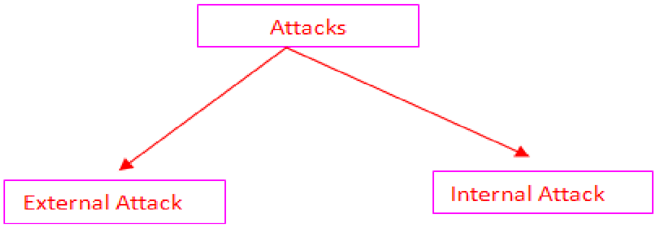
Fig (2):Attributes of Security

- AVAILABILITY A node should maintain its ability in order to provide all the designed services.
- INTEGRITY It guarantees the identity of messages sent when they are sent. Integrity may be altered by activity of malicious node or accidental altering by node C
- CONFIDENTIALITY Information access is possible only for authorized node.(ie) Confidentiality will be maintained in accessing messages by the way of providing privileges to authorized nodes
- AUTHENTICITY Providing assurance for the nodes which are participating in the communication and not the impersonators.
- NON-REPUDIATION It ensures that the sender cannot deny or repudiate that he has not send the message and receiver cannot deny or repudiate that he has not receive the message.
- AUTHORIZATION Authorization is a process in which an entity is issued a credential which privileges and permissions it has and cannot falsified y the certificate authority. It is also used to assign different access rights to different level of users.
- ANONYMITY It provides the all possible information that can be used to identify the owner or the current user of the node should be kept private and not be distributed by the node itself

V. 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:



Figure(3):Classification of Attacks

1. 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.

2. 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.

  Solution: Techniques of Frequency Hopping and Spread Spectrum Communication can protect the nodes from eavesdropping by preventing radio interface
- Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

  Solution: Traffic analysis can be avoided for any malicious node by supporting link layer security and securing wireless MAC protocol
- 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.

  Solution: Techniques of Frequency Hopping and Spread Spectrum Communication can protect the nodes from eavesdropping by preventing radio interface
- 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.

  Solution: Intrusion Detection System (IDS) is local module of intrusion detection for OLSR. This module does non-conformance evaluation of each node in network and reveals the existence of attack on routing protocol.
- 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.

  Solution: An approach HMTI (HELLO Message Timing Interval) finds nodes of attacker. HMTI has a profile of frequency which is set, a contravention in specification of OLSR protocol. The timing among packets becomes frequently bigger a lot as compare to the interval for legitimate node
- 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.

  Solution: The sequence number of destination should be adequately amplified by the node of attacker so that it looks authentic to source node. Ad hoc On Demand Distance Vector (AODV) is a scheme that finds out the black hole attack depending upon the received RREPs having difference in sequence numbers to destination
- 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.

  Solution: Use of Spread Spectrum Mechanism to block denial-of-service attacks could be a good solution.
- 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 thefirst phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

Solution: techniques proposed to detect and prevent gray-hole attack using multipath solution. J a technique based on alarm and alternate neighbor route mechanism is used. This is capable of detecting & preventing the single & cooperative malicious gray-hole nodes.

VI. CONCLUSION

We have classified the security attacks according to there characteristics and mentioned the solution for overcoming the attacks also .and for further studies we can survey on various other types of attacks other than that which is mentioned in the paper and also specify more other features, advantages, and its application to say where Manet can be used without any damages for user data during communication in a wirless network and also any algorithms which can be used in Manet for secure communication between nodes or users.

REFERENCES

[1] C.Siva Ram Murthy,B.S.Manoj,” Ad Hoc wireless networks Architectures and protocols” , Pearson Education, tenth impression, 2011

[2] A.Anna lakshmi Dr.K.R.Valluvan “A Survey of Algorithms for Defending MANETs against the DDoS Attacks”, Volume 2, Issue 9, September 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[3] H Yang H Y. Luo F Ye S W. Lu L Zhang “Security in mobile ad hoc networks: Challenges and solutions “ 2004 IEEE Wireless Communications.

[4] Y. Hu, A. Perrig, and D. Johnson, Ariadne: “A Secure On-demand Routing Protocol for Ad Hoc Networks,“ ACM MOBICOM, 2002.

[5] Sevil Şen, John A. Clark, Juan E. Tapiador Department of Computer Science, University of York, YO10 5DD, UK ”Security Threats in Mobile Ad Hoc Networks”

[6] Karlof C., Wagner D., “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Ad Hoc Networks, pp. 293-315, 2003

[7] Hu Y.-C., Perrig A., Johnson D.B., “Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks”, In Proc. of INFOCOM, 2003

[8] K. Sanzgiri et al., "A Secure routing Protocol for Ad Hoc Networks", In Proc. of the 10th IEEE Conference on Network Protocols, 2002

[9] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani “A Survey of Secure Mobile Ad Hoc Routing Protocols” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 10, NO. 4, FOURTH QUARTER 2008

[10] Priyanka Goya, Vinti Parmar, Rahul Rishi ,MANET: Vulnerabilities, Challenges, Attacks, ApplicationIJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011