Research Article Impact Factor: 0.621 ISSN: 2319-507X
Anup Deshmukh, IJPRET, 2014; Volume 2 (9): 330-336 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY GOALS AND ATTACKS IN MANET

ANUP V. DESHMUKH[1], RAHUL S. KALE[2], PROF. MS. V. M. DESHMUKH[2], NIKITA D. KALE[3]

1. Department of Information Technology, Prof. Ram Meghe Institute of Technology & Research, Badnera, (Amravati).India.
2. Department of Computer Science and Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera, (Amravati). India
3. Department of Computer Science and Engineering, G. H. Raisoni College of engineering, Nagpur, India

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: In the past few years, we have seen a rapid expansion in the field of mobile computing due to the proliferation of inexpensive, widely available wireless devices. However, current devices, applications and protocols are solely focused on cellular or wireless local area networks (WLANs), not taking into account the great potential offered by mobile ad hoc networking. A mobile ad hoc network(MANET) is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications.

Keywords: WLANNs, MANET, Sensor, Wireless Device.

Corresponding Author: MR. ANUP V. DESHMUKH

Access Online On:

www.ijpret.com

How to Cite This Article:

Anup Deshmukh, IJPRET, 2014; Volume 2 (9): 330-336

PAPER-QR CODE

INTRODUCTION

Ad hoc network are the temporary network. Ad hoc network short-range network and they are created when device uses the same protocol. Ad-hoc network does not need any subscription service. With the help of ad-hoc network it reduces the cost and improves the security. An ad hoc network is a local area network where messages flow from one node to another node instead of relying on a base station. Ad hoc networks give the ability to wireless devices to communicate with each other in local area network. Ad hoc networks decreased the dependence in infrastructure and increase the speed of deployment. Since nodes are not bound to any centralized control they are free to move about arbitrarily and hence the topology changes. Due to the noise, capacity of each link can vary. Ad hoc network nodes rely on batteries or some other exhaustive mean energy. For lean power consumption we tend to design these protocols. MANET [1],[2] stands for Mobile Ad hoc network. Mobile ad hoc network is a self-organized network of mobile nodes, without base station support. MANET consists of mobile nodes and a router. A router connects to multiple hosts and wireless communication devices. These wireless communication devices are transmitter or receivers. Receiver and transmitters will have smart antennas of various kinds and nodes (transmitter/receiver) can be fixed or mobile. In real life these node referred to those devices which are free to move in any direction such as a mobile phone, laptop, personal computer etc[6]. The paper organized as follows

In section 2 we explain overview of Mobile Ad-Hoc Network. In section 3 we explain Attcks in MANET. In section 4 we explain security goals. In section 5 we discuss the conclusion.

I. Overview of Mobile Ad Hoc Networks

In MANETs communication between nodes is done through the wireless medium. Because nodes are mobile and may join or leave the network, MANETs have a dynamic topology. Nodes that are in transmission range of each other are called neighbors.[2] Neighbors can send directly to each other. However, when a node needs to send data to another non-neighboring node, the data is routed through a sequence of multiple hops, with intermediate nodes acting as routers. An example ad hoc network is depicted in Figure 1. There are numerous issues to consider when deploying MANETs. The following are some of the main issues.

Fig 1: Example of mobile ad-hoc network

1. **Unpredictability of environment**: Ad hoc networks may be deployed in unknown terrains, hazardous conditions, and even hostile environments where tampering or the actual destruction of a node may be imminent. Depending on the environment, node failures may occur frequently.

2. **Unreliability of wireless medium**: Communication through the wireless medium is unreliable and subject to errors. Also, due to varying environmental conditions such as high levels of electro-magnetic interference (EMI) or inclement weather, the quality of the wireless link may be unpredictable. Furthermore, in some applications, nodes may be resource-constrained and thus would not be able to support transport protocols necessary to ensure reliable communication on a lossy link. Thus, link quality may fluctuate in a MANET.

3. **Resource-constrained nodes**: Nodes in a MANET are typically battery powered as well as limited in storage and processing capabilities. Moreover, they may be situated in areas where it is not possible to re-charge and thus have limited lifetimes. Because of these limitations, they must have algorithms which are energy-efficient as well as operating with limited processing and memory resources. The available bandwidth of the wireless medium may also be limited because nodes may not be able to sacrifice the energy consumed by operating at full link speed.

4. **Dynamic topology**: The topology in an ad hoc network may change constantly due to the mobility of nodes. As nodes move in and out of range of each other, some links break while new links between nodes are created. As a result of these issues, MANETs are prone to numerous types of faults including,

1. **Transmission errors**: The unreliability of the wireless medium and the unpredictability of the environment may lead to transmitted packets being garbled and thus received in error.

2. **Node failures**: Nodes may fail at any time due to different types of hazardous conditions in the environment. They may also drop out of the network either voluntarily or when their energy supply is depleted.

3. **Link failures**: Node failures as well as changing environmental conditions (e.g., increased levels of EMI) may cause links between nodes to break.

4. **Route breakages**: When the network topology changes due to node/link failures and/or node/link additions to the network, routes become out-of date and thus incorrect. Depending upon the network transport protocol, packets forwarded through stale routes may either eventually be dropped or be delayed; packets may take a circuitous route before eventually arriving at the destination node.

5. **Congested nodes or links**: Due to the topology of the network and the nature of the routing protocol, certain nodes or links may become over utilized, i.e., congested. This will lead to either larger delays or packet loss. Routing protocols for MANETs must deal with these issues to be effective

II. 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.[3]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:

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.

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.[4] 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.

3.6 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.

3.7. 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.

3.8 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.

3.9Man- 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.

3.10 Gray-hole attack: This attack is also known as routing miss behaviour 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.

III. Security Goals

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. [5] 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

4.1 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.

4.2 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[3].

4.3 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.

4.4 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 because only the legitimate sender can produce a message that will decrypt properly with the shared key.

4.5 Non repudiation: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

4.6 Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

4.7 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].

IV. CONCLUSION

The rapid evolution in the field of mobile computing is driving a new alternative way for mobile communication, in which mobile devices form a self-creating, self-organizing and self-administering wireless network, called a mobile ad hoc network. Its intrinsic flexibility, lack of

infrastructure, ease of deployment, auto-configuration, low cost and potential applications make it an essential part of future pervasive computing environments.

REFERENCES

1. Bai F., Sadagopan, N., Krishnamachar ,B., Helmy, A. (2004)"Modeling Path Duration Distributions in MANETs and Their Impact on Reactive Routing Protocols" IEEE Journal on Selected Areas in Communication ,Vol. 30 Issue 11, pp. 1357-1373.

2. Wu, J., Dai, F., Gao, M., Stojmenovic, I.(2002),"On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks" Journal Of Communications And Network, Vol. 4 Issue 1.

3. 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

4. Humayun Bakht," *Survey of Routing Protocols for Mobile Ad-hoc Network*", International Journal of Information and Communication Technology Research, 258-270, October 2011

5. Hongmei Deng, Wei Li, and Dharma P. Agrawal, *"Routing Security in Wireless Ad Hoc Networks"* IEEE Communications Magazine October 2002

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

7. Raja ram, A. Dr. and Sugesh, J. (2011),"Power Aware Routing for MANET Using On demand Multipath Routing Protocol". IJCSI International Journal of Computer Science, Vol. 8 Issue 2, pp. 517-522.

8. Wu, J., Dai, F., Gao, M., Stojmenovic, I.(2002),"On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks" Journal Of Communications And Network, Vol. 4 Issue 1.

9. Zhang, j., Zhang Q., Li, B , Luo, X., Zhu, W. (2006),"Energy-Efficient Routing in Mobile Ad Hoc Networks: Mobility-Assisted Case" IEEE Transaction On Vehicular Technology, Vol. 55 Issue 1, pp. 369-379.

10. Zhu, Z. Chen, X., ji. F.,Zhang, L., Farahmand, F., Jue, P.,Jason.(2012),"Energy-Efficient Translucent Optical Transport Networks With Mixed Regenerator Placement" Journal of light wave technology, Vol. 30 Issue 19, pp. 3147-3156.