RESEARCH PAPER | Information Technology | Volume : 3 | Issue : 1 | January 2013 | ISSN - 2249-555X

Challenges in Mobile Ad Hoc Networks: Security Threats and its Solutions

KEYWORDS: Mobile Ad Hoc Network, Challenges, Security, Denial of Service (DoS)

Miss Dhara N. Darji
Assistant Professor, DCS, Ganpat University.

Miss Nita B. Thakkar
Assistant Professor, DCS,Ganpat University.

ABSTRACT *A Mobile Ad Hoc Network (MANET) is a self-organizing, infrastructureless, multi -hop network. The wireless and distributed nature of MANETs poses a great challenge to system security designers. A number of challenges like open peer-to-peer network architecture, stringent resource constraints, shared wireless medium, dynamic network topology etc. are posed in MANET. As MANET is quickly spreading for, security challenges have become a primary concern to provide secure communication. In this paper, we are trying to analyze and study the MANET characteristics, challenges and also identify the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks in each layer.*

I. Introduction

A MANET is a self-organizing collection of wireless mobile nodes that form a temporary and dynamic wireless network without any infrastructure. MANETs are self-configuring; there is no central management system with configuration responsibilities. All the mobile nodes can communicate each other directly, if they are in other's wireless links radio range [1][2].

The mobile ad hoc networks are different from Internet in two major ways. The first is that the hosts in this network are resource-constrained. They have only limited energy, computing power and memory. The second is that the hosts (and therefore the routers) of the network are mobile and the topology changes rapidly. These two features pose great challenges to the researchers working in the area [3].

MANET nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility [4]. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network [6].

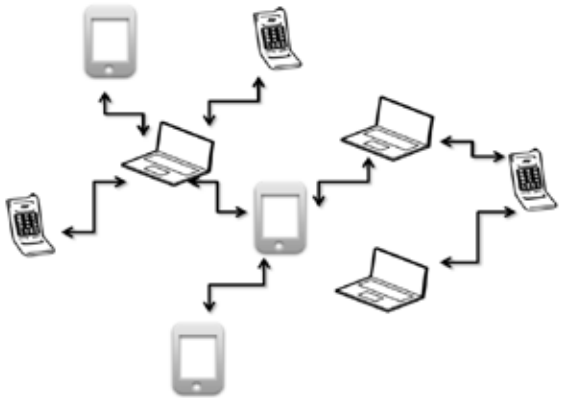

Figure 1: Mobile Network

II. Characteristics of MANET

√ Network is not depending on any fix infrastructure for its operation.
√ Multi-hop routing
√ Dynamic network topology
√ Device heterogeneity
√ Bandwidth constrained variable capacity links
√ Limited physical security
√ Network scalability
√ Self-creation, self-organization and self-administration

III. MANET Challenges

The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design.

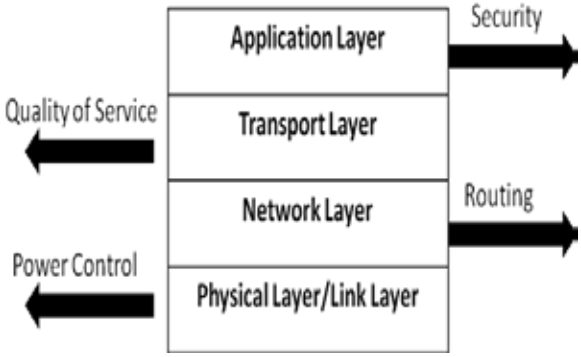

Figure 2: MANET Challenges [6].

• Absence of Infrastructure :
Ad hoc networks operate independently of any infrastructure, which makes inapplicable any classical solutions based on certification authorities and on line servers. In which there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network, means it is self-evident. [1][6].

• Lack of Centralized monitoring :
Absence of any centralized monitoring makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly and large scale ad hoc network . It is rather common in the ad hoc network that benign failures such as transmission impairments and packet dropping.

• Security and Reliability :
An ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets in spite of accumulation to the frequent vulnerabilities of wireless connection. Additionally wireless link features commence also reliability problems, because of the restricted wireless transmission range, data transmission errors, the broadcast nature of the wireless medium and mobility-induced packet losses.

• Poor Transmission Quality :
Communication links in an ad hoc network are unstable such that running conventional protocols for MANETS over a high loss rate will suffer from severe performance degradation.

Volume : 3 | Issue : 1 | January 2013 | ISSN - 2249-555X

However, with high error rate, it is very much difficult to deliver a packet to its destination [13].

• Dynamically changing network topology :
Nodes are free to move arbitrarily. The network topology may change randomly and have no restriction on their distance from other nodes. As a result of this random movement, the whole topology is changing in an unpredictable manner, which in turn gives rise to both directional as well as unidirectional links between the nodes.

• Power Consumption :
Due to mobility of nodes in the ad hoc network, nodes will rely on battery as their power supply method [1][9]. Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device. By increasing the power and processing ability makes the nodes bulky and less portable. So only MANET nodes has to optimally use this resource

• Limited physical security :
Mobile wireless networks are generally more prone to physical security threats than a fixed- cable nets or a shared wireless medium accessible to both legitimate network users and malicious attackers. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered [11]. Existing link security techniques are often applied within wireless networks to reduce security threat.

IV. Security Attacks in Mobile Ad Hoc Wireless
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. The current Mobile ad hoc networks allow for many different types of attacks.

There are two types of security attacks:-

a. Basic security attacks in Mobile Ad Hoc Wireless Networks
They are also classified into two types:

♦ **Active Attacks**
Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious. Active attacks involve actions such as the replication, modification and deletion of exchanged data

♦ **Passive Attacks**
Passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

b. Other types of possible security attacks in Mobile Ad Hoc Wireless Networks
These attacks can be grouped in: Denial of service, Eavesdropping, Impersonation and Routing Attacks.

♦ **Denial of service**
√ The intruder use the radio jamming method to conduct DoS attacks means attempts to utilize batteries of other nodes by requesting routes. [7][8]
√ The intruder use the battery exhaustion methods to conduct DoS attacks means also keeps busy other nodes by forwarding unnecessary packets[7][8]

♦ **Eavesdropping**
The goal of eavesdropping is to obtain some confidential information that should be kept secret during the communication. [9] The confidential information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

♦ **Impersonation**
As there is no authentication of data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network and alters the target of the network topology that a benign node can gather [7].

♦ **Routing Attacks**
√ Generating fake Route Error to interrupt a working route.
√ Impersonating another node to spoof route message.
√ Advertising a false route metric to misrepresent the topology.
√ Suppressing Route Error to mislead others.
√ Sending a route message with wrong sequence number to suppress other legitimate route messages.
√ Flooding Route Discover excessively as a Denial of Service attack.
√ To introduce a false route it modifying a Route Reply message.

Security Attacks on each layer in MANET [7]

Layer	Attacks
Application layer	Repudiation, Data Corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, Blackhole, Byzantine, Flooding, Resource Consumption location disclosure attacks
Link layer	Traffic analysis, Monitoring, Disruption MAC (802.11), WEP weakness
Physical layer	Jamming , Interceptions, Eavesdropping

Security Issues for MANET [7] [10]

Layer	Security issues
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating and securing end-to-end communications through data encryption
Network layer	Protecting the ad hoc routing and forwarding protocols
Link layer	Protecting the wireless MAC protocol and providing link-layer security support
Physical layer	Preventing signal jamming denial-of-service attacks

Mobile Ad Hoc Networks Security Solutions
The ultimate goals of the security solutions for MANETs are to provide security services. There are six main security services for MANETs.

Security services
√ **Authentication**
Authentication means that correct identity, that essentially assurance that participants in communication are genuine and ensures that the access and supply of data is done only by the authorized parties. Among all the security services, authentication is probably the most complex and important issue in MANETs since it is the bootstrap of the whole security system.

√ **Confidentiality**
Confidentiality means certain message information is only readable or accessible by the authorized party. Once authentication is achieved in MANET, confidentiality is a matter of encrypting the session using whatever key material the communicating party agrees on

√ **Integrity**
Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted

√ **Nonrepudiation**
Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message.

Volume : 3 | Issue : 1 | January 2013 | ISSN - 2249-555X

√ **Anonymity**

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities [9]

√ **Availability**

Availability means the normal service provision in face of all kinds of attacks. [15] The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [9]. Denial-of-service attacks mainly challenge the security criteria, where every nodes in the network can be the attack intention and thus some selfish and malicious nodes make some of the network resources and services occupied, for e.g.:- the key management service.[8]

REFERENCE [1] G. Santhi and Alamelu Nachiappan, "A SURVEY OF QOS ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS" International journal of computer science & information Technology (IJCSIT) Vol.2, No.4, August 2010 | [2] UMANG SINGH, "SECURE ROUTING PROTOCOLS IN MOBILE ADHOC NETWORKS-A SURVEY AND TAXANOMY" International Journal of Reviews in Computing, 30th September 2011. Vol. 7 | [3] Qunwei Zheng, Xiaoyan Hong, and Sibabrata Ray, "Recent Advances in Mobility Modeling for Mobile Ad Hoc Network Research",2004. | [4] Stephen Mueller, RoseP.Tsang, and Dipak Ghosal," Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges". | [5] Pravin Ghosekar, Girish Katkar, Dr. Pradip Ghorpade," Mobile Ad Hoc Networking: Imperatives and Challenges", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010. | [6] B.SOUJANYA, T.SITAMAHALAKSHMI, CH.DIVAKAR "STUDY OF ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS", B.Soujanya et al. / International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 4 April 2011. | [7] Anuj Joshi, Pallavi Srivastava and Poonam Singh, "Security Threats in Mobile Ad Hoc Network", S-JPSET : ISSN : 2229-7111, Vol. 1, Issue 2, samriddhi, 2010 | [8] Krishan Kant Lavania, G. L. Saini, Kothari Rooshabh H., Yagnik Harshraj A., "Privacy Anxiety and Challenges in Mobile Ad Hoc Wireless Networks and its Solution", International Journal of Scientific & Engineering Research Volume 2, Issue 9, September-2011, ISSN 2229-5518. | [9] Wenjia Li and Anupam Joshi, "ecurity Issues in Mobile Ad Hoc Networks - A Survey". | [10] H Yang, H Y. Luo, F Ye, S W. Lu, L Zhang "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications. February 2004. | [11] Kavita Taneja and R. B. Patel, "Mobile Ad hoc Networks: Challenges and Future", Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT-2007) RIMT-IET, Mandi Gobindgarh. March 23, 2007. | [12] Fei Hu, Neeraj K. Sharma, "Security considerations in ad hoc sensor networks" 2005. | [13] G. S. Mamatha and Dr. S. C. Sharma, "ANALYZING THE MANET VARIATIONS, CHALLENGES, CAPACITY AND PROTOCOL ISSUES", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010 | [14] Eroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges" | [15] Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen, "A security architecture for Mobile Ad Hoc Networks" |