ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

# Analytical Study on Security Issues in Mobile Ad-Hoc Network

[1]N.Kowsalya, [2]M.Karthika, [3]N.Boomathi

[1]Professor, Department of Computer Science And Application, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, Tiruchengode, Namakkal, India

[2,3]Fulltime M.phil Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women, Elayampalayam, Tiruchengode, Namakkal, India

**ABSTRACT**: A Mobile Ad hoc Network (MANET) consists of movable platforms which are free to move arbitrarily. The flexibility of mobile ad hoc network introduces new security threats. Many conventional security solutions used for wired networks are ineffective and inefficient for the highly dynamic and resource-constrained environments where use of MANET may be predictable. We first analyze the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. In this paper, we generally focus on the security issues and challenges in the mobile ad hoc networks.

**KEY WORDS**: Security Issue, Attacks, MANET, Proactive protocol, Reactive Protocol.

## I. INTRODUCTION

A Mobile Ad hoc network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

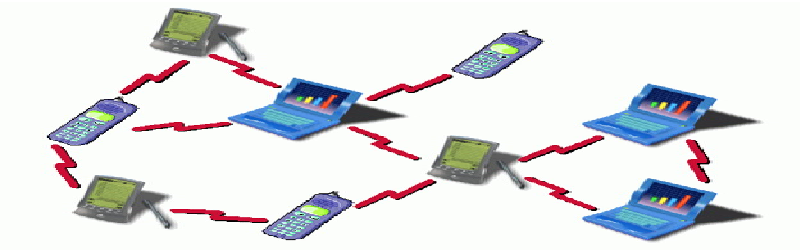

Fig.1. Nodes in the MANET

## II. SUSCEPTIBILITIES OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

**a) Lack of Secure Boundaries**
The meaning of this vulnerability is self-evident: 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.

This vulnerability originates from the nature of the mobile ad hoc network: freedom to join,leave and move inside the network. In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets [6].

However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the so-called secure boundary to protect the network from some potentially dangerous network accesses. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, leakage of secret information, data tampering, message replay, message contamination, and denial of service [4].

**b)Unreliability of wireless links between nodes**
Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

**c)Dynamic topologies**
Nodes are free to move arbitrarily; thus, the network topology- -which is typically multi hop--may change randomly and rapidly at unpredictable time. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the routing protocol.

**d)Lack of Centralized Management Facility**
Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Due to absence of centralized management facility problems detection of attacks, path breakages, transmission impairments and packet dropping, breakage of the cooperative algorithm take place because decision making process is decentralized.

## III. CHARACTERISTICS OF MANET

Dynamic Topologies:
Nodes are free to move randomly with different speeds; thus, the

- network topology may change randomly and at unpredictable times. Energy Constrained Operation: - Some or all of the nodes in an ad hoc network may rely
- on batteries or other exhaustible means for their energy. For these nodes, the most important system design optimization criteria may be energy conservation. Limited Bandwidth: - Wireless links continue to have significantly lower capacity than
- infrastructure networks. In addition, the realized throughput of wireless communications – after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate. Security Threats: - Mobile wireless networks are generally more prone to physical
- security threats than fixed- cable nets. The increased possibility of eavesdropping, spoofing, and minimization of denial-of-service type attacks should be carefully considered. [2]

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

## IV. SECURITY ATTRIBUTES

Security of a MANET can be inspecting by analyzing the certain attributes. These are:

**a)Availability**
The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it [4]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [5].

b) **Integrity**
Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [9]:

- Malicious altering
- Accidental altering

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

**c)Confidentiality**
Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

**d)Authenticity**
Authenticity is essentially assurance that participants in communication are genuine and not impersonators [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

**e)Nonrepudiation**
Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

**f)Authorization**
Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

**g)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.

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

## V. SECURITY SCHEME

There are basically two approaches to securing a MANET: proactive and reactive. The proactive approach attempts to thwart security threats in the first place, typically through various cryptographic techniques. On the other hand, the reactive approach seeks to detect threats a posteriori and react accordingly. Each approach has its own merits and is suitable for addressing different issues in the entire domain. For example, most secure routing protocols adopt the proactive approach in order to secure routing messages exchanged between mobile nodes, while the reactive approach is widely used to protect packet forwarding operations[5] [11]. MANET routing protocols as shown in fig.2

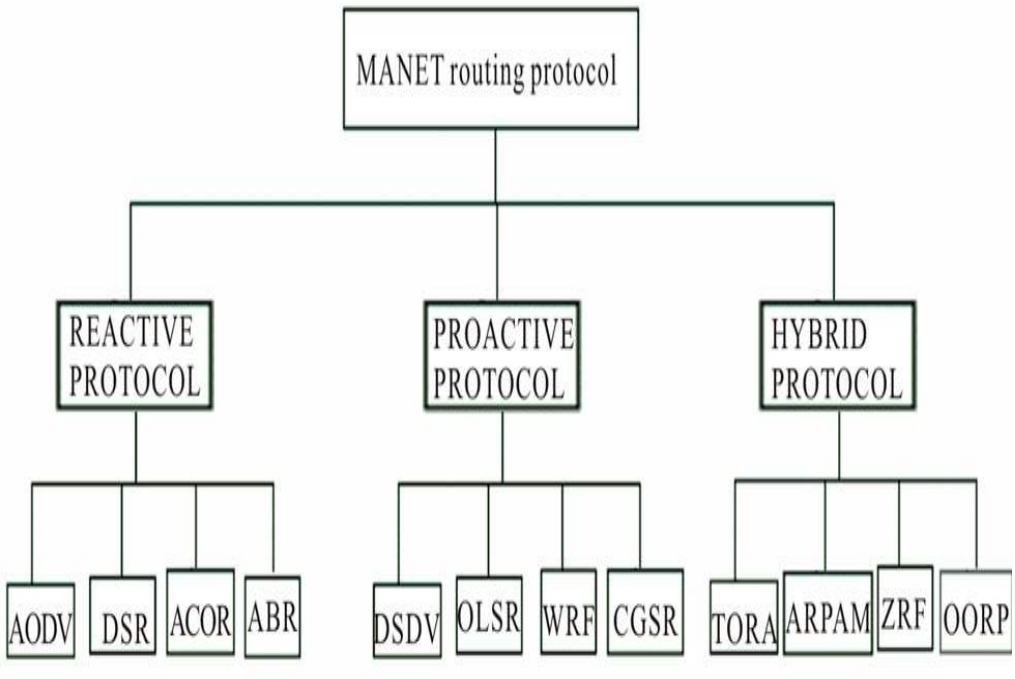


Fig.2 MANET routing protocol

**a) Defense Method against Wormhole Attacks**

Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks [9]. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and replays them there into the network. The replay of the information will make great confusion to the routing issue in mobile ad hoc network because the nodes that get the replayed packets cannot distinguish it from the genuine routing packets. A packet leash as a general mechanism for detecting and, thus defending against wormhole attacks.

A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. There are two main leashes, which are geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed-of-light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows.

A geographical leash in conjunction with a signature scheme (i.e., a signature providing no repudiation), can be used to catch the attackers that pretend to reside at multiple locations: when a legitimate node overhears the attacker claiming

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

to be in different locations that would only be possible if the attacker could travel at a velocity above the maximum node velocity v, the legitimate node can use the signed locations to convince other legitimate nodes that the attacker is malicious

**b) Defense against black hole attacks**

Security-Aware Routing Protocol (SAR) is used. A security metric or trust level added into the RREQ. In the intermediate nodes if trust level is satisfied the node will process the RREQ. The destination generates RREP with the specific security metric.

To prevent identity theft stronger access control mechanism is required. 3. Defense against impersonation and repudiation attack ARAN provides authentication and nonrepudiation services using predetermined cryptographic certificates for end-to-end authentication. Each hop verifies the signature of the previous hop and replaces it with its own. Fig [3]

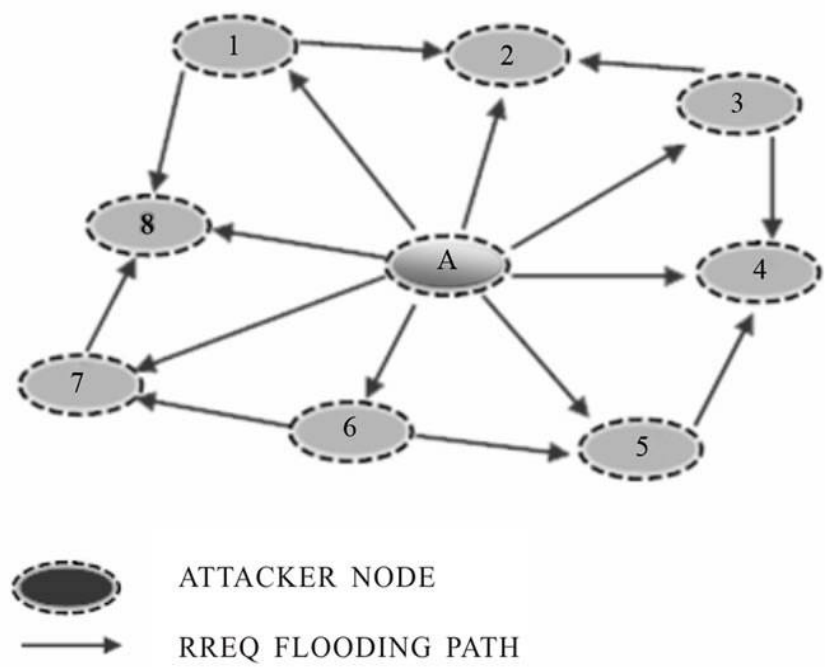


Fig.3 Process of RREQ

**c) Secure AD-HOC Routing approach using Localize Self healing Communities**

The concept of "self-healing community" is based on the observation that wireless packet forwarding typically relies on more than one immediate neighbor to relay packets. Community based security explores node redundancy at each forwarding step so that the conventional per-node based forwarding scheme is seamlessly converted to a new per community based forwarding scheme. Since a self-healing community is functional as long as there is at least one cooperative "good" node in the community, there is no requirement that how many nodes in the community should be available to provide reliable packet forwarding services. There are one configuration and one reconfiguration protocol that can respectively be used to initially set up the self-healing community and fix the community if there is a shape loss due to the mobility or change of topology.

**d)Intrusion Detection Techniques**

An Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [5]. Each mobile node runs an IDS agent independently. It has to observe the behavior of neighboring nodes, detect local intrusion, Cooperate with neighboring nodes, make decisions and take actions. [12]

ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 6, June 2016**

## VI. CONCLUSION

Importance of MANET cannot be denied as the world of computing is getting portable and compact. In this survey paper we discussed some typical and dangerous vulnerability in the MANET, attack types security criteria, which act as a guidance to the security-related research works in this area.

### REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
[2] De Morais Cordeiro, Carlos, and Dharma P. Agrawal "Mobile Ad Hoc Networking" Center for Distributed and Mobile Computing, ECECS, University of Cincinnati (2002).
3. S.Madhavi and Tai Hoon Kim, "An Intrusion Detection System in Mobile Adhoc Networks", International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.
[4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
[5] Lidong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security, November/December 1999.
[6] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.
[7] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003.
[8]Data Integrity, from Wikipedia, the free encyclopedia,[Online] Availlable: http://en.wikipedia.org/wiki/Data_integrity.
[9] Y. Hu, A. Perrig, D. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks", in Proceedings of ACM MOBICOM'02, 2002.
[10] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. BeldingRoyer, "A Secure Routing Protocol for Ad Hoc Networks", in Proceedings of ICNP'02, 2002.
[11] L. Zhou, Z. J. Haas, "Securing Ad Hoc Networks", IEEE Networks, Volume 13, Issue 6 1999.
[12] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Adhoc Networks", in Proceedings of the 6th International conference on mobile computing.