Asian Journal of Information Science and Technology (AJIST)
Vol.4.No.1. 2016 pp 7-11
available at: www.goniv.com
Paper Received :08-04-2016
Paper Accepted:22-04-2016
Paper Reviewed by: 1. R. Venkatakrishnan 2. Dr.G.Ramesh
Editor:Prof.P.Muthukumar

A SURVEY ON SECURITY ISSUES IN MANET: CHALLENGES, ATTACKS, AND SOLUTIONS

Joyshyajit Leiharungbam[1], Mrs.K.Adlin Suji[2], Mr.M.Rajakumar[3]
[1]PG Student, Department of MCA, Dhanalakshmi Srinivasan Engineering College, Perambalur, India
[2]Associate Prof., Department of MCA, Dhanalakshmi Srinivasan Engineering College, Perambalur, India
[3] Prof., Head, Department of MCA, Dhanalakshmi Srinivasan Engineering College, Perambalur, India

ABSTRACT

A mobile ad-hoc network (MANET) is a self-organizing and self-managing system without fixed infrastructure or centralized Administration where its mobile nodes are communicate with each other through wireless links with radio frequency, it has special characteristics like open network boundary, dynamic topology and hop-by-hop communications, MANET faces variety of challenges to make reliable and secured communication, among those challenges security has become a primary concern in MANET environment. In this paper we discuss security issues, attacks and challenges present in MANET. Finally we survey the current security solutions for the MANET.

Index Terms—MANET, security, challenges, attacks, solutions

I. INTRODUCTION

Ad-hoc mode is one of the networking topologies provided in the 802.11 standard. It consists of at least two wireless stations or nodes where no access point is involved in their communication. Ad-hoc mode WLANs are normally less expensive to run, as no APs are needed for their communication. A MANET is a wireless network without any fixed infrastructure, formed by a set of mobile hosts that dynamically establish their own network on the fly, without relying on any central administration. Mobile nodes used in MANET have to ensure the roles that were ensured by the powerful fixed infrastructure in traditional networks. This is a challenging task, since mobile nodes have limited resources (CPU, storage, energy, etc.). Moreover, the MANET environment has some features that add extra complications, such as energy-constrained of the nodes, the frequent topology changes caused by nodes mobility, the unreliability and the bandwidth limitation of wireless channels. However, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment[1]. It is also true that existing security solutions for wired networks do not directly apply to the Mobile ad hoc networks domain. In MANET, it is much more vulnerable to attacks than a wired network due to its limited physical security, volatile network topologies, power-constrained operations, lack of centralized monitoring and management point.

II. SECURITY CHALLENGES IN MANET

Security challenges which we are commonly found in MANET are as follows:

A. 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.

B. Confidentiality

Confidentiality ensures that certain information is accessed only by authorized parties. It is to maintain confidentiality of some confidential information; we need to keep them secret from all entities that do not have privilege to access them, sometimes it is called secrecy or privacy.

C. Integrity

Integrity means that assets can be modified only by authorized parties or only in authorized way. Integrity assures that a message being transferred is never corrupted. Integrity can be compromised mainly in two ways [11]:

- Malicious altering, and
- Accidental altering

D. Authentication

Authentication enables a node to ensure the identity of peer node it is communicating with and it is essentially assurance that participants in communication are authenticated and not impersonators. However, in MANETs, there is no central administration so it is difficult to authenticate an entity.

E. 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. It is generally assigns different access rights to different types of users. For example, a network management can be performed by network administrator only.

III. SECURITY ATTACK IN MANET

Attacks in MANET are divided according to their origins or their nature. Origin based classification splits attacks into two categories; external and internal, whereas, nature based classification splits them up into passive attacks and active attacks

***External attacks*:** This category Includes attacks launched by a node that do not belong to the logical network, or is not allowed to access to it.

***Internal attacks*:** This category includes attacks launched by an internal compromised node; it is a more several kind of threat to the network since the proposed defence toward external attacks is ineffective against compromised and internal malicious nodes [3].

***Passive attacks*:** A passive attack attempts to retrieve valuable information by listening to traffic channel without proper authorization, but does not affect system resources and the normal functioning of the network. This attack is a continuous collection of information; this information would be used later when launching an active attack

***Active attacks*:** An active attack attempts to change or destroy the system resources. It Includes almost all the other attacks launched by actively interacting with victims, like sleep deprivation torture that aims the batteries charges, hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them, jamming, that causes channel unavailability, attacks against routing protocols, etc..

A. Denial-Of-Service Attack

Denial-Of-Service (DoS) attack is characterized by an explicit attempt to prevent legitimate users of a service from using that service. The attackers exactly use the radio jamming and battery exhaustion methods to conduct DoS attacks to the MANET to the two vulnerabilities. In this attack, a specific node or service will be inaccessible and network resources like bandwidth will be wasted, and packet delay and congestion increases.

B. Impersonation

If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. This attack is a severe threat to the security of mobile ad hoc network [2].

C. Eavesdropping

Eavesdropping attack is also usually happens in the mobile ad hoc networks. This is a passive attack, the node simply observes the confidential information, and this information can be later used by the malicious node. The confidential information like location, public key, private key, password etc. can be fetched by eavesdropper.

D. Routing Attacks

The main influences brought by the attacks against routing protocols include network partition, routing loop, resource deprivation and route hijack [14]. There are two main attack strategies in this type: one is selfishness and another is denial-of-service.

E. Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network and tunnels them to another point in the network, and then replays them into the network from that point. Fault routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole [13].

F. Replay Attack

This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions

G. Jamming

In jamming, attacker primarily keeps examining the wireless medium in order to determine frequency at which receiver node is receiving signal from sender. It then transmits signals on that frequency so that error free receptor is hindered

IV. SECURITY SOLUTIONS IN MENET

The security solutions are mainly based on network protection and raising the level of security in the Mobile ad-hoc network.

A. Authentication during all phases

Authentication techniques are used to excluding attackers or unauthorized nodes to participate in the routing. Most of the solutions rely on Certificate Authority (CA) presence. In Many solution the use of a trusted certificate server where public key is priory known to all valid nodes within the network; this renders the solution centralized and less flexible [13].

B. Secure neighbour detection

This solution overcomes the illegal use of high power range to launch the rushing attacks in network. Since the sender using higher powers cannot receive the packet from further nodes, and it will not be able to perform the neighbour node detection process, then their packets will be ignored by these nodes [8].

C. End-to-end Security Association (SA)

Security association or trust relationship can be instantiated, for example, by the knowledge of the public key of each other. This SA prevents malicious from Injecting forged data packets[3].

D. Broadcasting Approaches in MANET

In Mobile ad-hoc network (MANET), a number of broadcasting approaches on the basis of cardinality of destination set [10]:

- Unicasting
- Multicasting
- Broadcasting
- Geocasting

V. CONCLUSION

In wireless network, there are many security challenges in designing and also many security solutions have developed. However, the existing wireless network security solutions cannot be implemented in mobile ad-hoc network environment. As node are mobility and the nature of free infrastructure lead to many more security challenges in designing for it. In this survey paper, we have studied about security issues in the MANET environment by taking challenges, attacks and current solutions. Moreover, security solutions cannot be implemented in a better way in Mobile ad hoc networks due to its mobility and free infrastructure nature, also challenges exist in designing part, so as a continuation of our work we will implement a better security solution to prevent from those attacks with acknowledgement based packets transmission for MANET. In future work, we need to keep concentrate on the secure routing protocol which can prevent from those intruders in the network, to make an eco-friendly Mobile ad-hoc network.

VI. REFERENCES

[1] Dr.Nabeel Zanoon, Dr.Nashat Albdour, Dr.Hatem S. A. Hamatta, and RashaMoh'd Al-Tarawneh," SECURITY CHALLENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS, AND SECURITY SOLUTIONS", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015.

[2] CDMA Development Group, "3G - CDMA2000 1xEV-DO Technologies," http://www.cdg.org/technology/3g 1xEV-DO.asp. Last accessed April 2009.

[3] Panagiotis Papadimitratos and Zygmunt J. Haas. Secure data transmission in mobile ad hoc networks. In the 2003 ACM workshop on Wireless security, San Diego, CA, USA, session: Secure routing, pages 41{50, 2003.HAO YANG, HAIYUN LUO, FAN YE, SONGWU LU, AND LIXIA ZHANG, UCLA COMPUTER SCIENCE DEPARTMENT," SECURITY IN MOBILE AD HOC NETWORKS: CHALLENGES AND SOLUTIONS", IEEE Wireless Communications • February 2004, pages 38-47.

[4] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[5] Sevil Şen, John A. Clark, Juan E. Tapiador," Security Threats in Mobile Ad Hoc Networks"

[6] Priyanka Goyal, Vinti Parmar, Rahul Rishi,"MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893 www.IJCEM.org, page 32-37.

[7] Yih-Chun Hu, Adrian Perrig, and David B. Johnson,"Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceeding of the ACM workshop on WIreless Security", WISE 2003, San diego, CA, USA, september 2003.

[8] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth Belding-Royer,"A secure routing protocol for ad hoc networks". In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP 02), November 2002.

[9] IIyas, M., 2003. The hand book of ad -hoc wireless networks. CRC press LLC.

[10] Yi-Chun Hu and Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, pp.28-39, Vol.2, No.3, 2004, http://dx.doi.org/10.1109/MSP.2004.1

[11] Monika, Mukhesh Kumar, Rahul Rishi," Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review", International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010.

[12] Z.A.Khan and M. H. Islam, "Wormhole attack: A new detection technique," presented at the international conference on Emerging Technologies (ICET), 2012.

[13] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth Belding-Royer. A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP 02), November 2002.

[14] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.