Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 92 (2016) 329 – 335

Procedia Computer Science

2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016)

Srikanta Patnaik, Editor in Chief

Conference Organized by Interscience Institute of Management and Technology

Bhubaneswar, Odisha, India

Security Issues In Mobile Ad Hoc Networks

Sarika S[a*], Pravin A[b], Vijayakumar A[c], Selvamani K[d]

[a,] Assistant Professor, Department of Computer Science and Engineering, Sathyabama University,Chennai, India
[b]Assistant Professor, Department of Computer Science and Engineering, Sathaybama University,Chennai, India
[c]Professor, Department of Information Technology, Jerusalem College of Engineering, Anna University, Chennai, India
[d]Assistant Professor, Department of Computer Science and Engineering, Anna University, Chennai, India.

Abstract

In wired networks, there are lots of protections while communication occurs. In these networks, the intruders are pass through the firewalls and secured gateways for safe and secured communications. Moreover, the wired networks ensure the secured communications. But, in the case of wireless mobile ad hoc networks, the nodes are dynamic and the topology based and also needs more power consumptions. Because of mobility in wireless mobile adhoc networks, also there are lots of vulnerabilities when the attackers wish to collapse the partial or entire networks. Hence, there are lots of requirement for an understanding of the various problems associated with the wireless mobile networks. In this paper, the various vulnerabilities, attacks and security mechanisms are discussed for mobile ad hoc networks (MANETs) in detail.

Keywords: Attacks, Intrusion, Mobile ad hoc networks, Security, Vulnerability, Wireless networks

doi:10.1016/j.procs.2016.07.363

*Sarika.S, Phone: :+91-99410-15077 ; *E-mail address* :sarikajanani@gmail.com

1. Introduction

Mobile Ad hoc Networks(MANETs) refers the one kind of mobile networks encompass the wireless mobile nodes for communication. These nodes organize themselves dynamically in random and volatile topologies. In such a scenario, a wireless system which can deliver information from a source to destination, considering the mobility of the nodes in mind, is crucial. It is so, because a node can receive a packet of data that is sent within it's frequency range. So, when the nodes are mobile, the receiving node can move out of frequency range at anytime. It allows people and devices to inter network in areas with no pre-existing communication infrastructure.

The main characteristics of MANETs are [1]

1. Self-organizing and self-managing
2. Most or all of the nodes are mobile
3. Network topology changes
4. Wireless
5. Node is both a host and a router
6. Multiple hop routing
7. Power constraint
8. Variation in scale
9. Heterogeneity
10. Decentralization
11. Variable routing paths
12. Dynamic topology
13. No access point required
14. Distributed Operation

MANETs are used in the following areas

1. Military Battlefield
2. Sensor Networks
3. Commercial Sector
4. Medical Service
5. Personal Area Network

1. SECURITY GOALS

2.1. *Availability*

A node always provides the services it is designed for. It concentrates crucially on denial-of-service attacks. Some selfish nodes make some of the network services unavailable [2].

2.2. *Integrity*

Integrity refers to the process of guaranteeing the identity of the messenger. There are two challenges - malicious attack, and accidental altering. The main difference between these two is the intent. In malicious attack, the attacker intentionally changes information, whereas in accidental altering, alteration is accidentally done by a benign node.

2.3. *Confidentiality*

Sometimes, some information are ought to be accessible only to a few, who has been authorized to access it. Others, who are unauthorized, shouldn't be able to get a hold of this confidential information.

2.4. *Authenticity*

Authenticity checks if a node is an impersonator or not [1]. It is imperative that the identities of the participants are secured by encrypting their respective codes. The adversary could impersonate a benign node and can gain access to confidential resources or even distribute some harmful messages.

2.5. *Non-Repudiation*

Non-repudiation ensures that the sender and the receiver of a message cannot deny sending or receiving such a message. The instance of being compromised is established without ambiguity. For example, if a node recognizes that the message it has received is erroneous or genuine. The node can then use the incorrect message as a proof to notify the other nodes that the node should have been compromised.

2.6. *Authorization*

A bonafide credentials to be issued by the appropriate authority which will be mandatory to assign access rights to users, at different levels. It usually uses an authorization process.

2.7. *Anonymity*

It refers to information that is used to identify the owner. The current user has to be kept confidential and not be distributed. It is very similar to the privacy preserving.

3. VULNERABILITIES

3.1. *No Secure Boundaries*

In a wired network, adversaries have to get physical access to the network medium. They may even have to go through layers of firewall and gateway. But, in MANETs, it is easy to gain access to the network, provided the node is in frequency range[3]. Thus, MANETs do not provide secure boundary[1].

3.2. *Power and Computational L imitations*

Wired networks can get electric power supplies, but in the case of wireless network, there is restricted power supply. Thus, any node in a network may act selfish, if it has limited power supply[3].

3.3. *Lack of Centralized Management Facility*

Ad hoc networks do not have a central mechanism that is used for management, leading to some vulnerable problems [1]. The lack of centralized management machinery makes the identification of attacks a very difficult problem as it is not easy to check and control the traffic in a highly dynamic and large-scale ad hoc network.

3.4. *Cooperativeness*

The common assumption about routing algorithms in MANETs is that the nodes are cooperative and non-malicious. Thus, a malicious attacker can easily become an essential routing agent and interrupt network operations by disobeying the protocol specifications.

4. ATTACKS

4.1. *Active*

Active attacks are the attacks that are performed by the malicious nodes. Moreover, these nodes consume some energy in order to perform the attacks. Active attacks involve some changes of data or creation of false information. The following attacks come under the category of active attacks:

4.1.1. *Sink holes*

A compromised node tries to attract the data to it, from all neighbouring nodes. The node eavesdrops on all the data that is being communicated among its neighbouring nodes. Sinkhole attacks can also occur on ad hoc networks such as AODV by using techniques like maximizing the sequence number or minimizing the hop count.

4.1.2. *Denial of Service*

The DoS attacks are performed by flooding some kind of network traffic to the target. This exhausts the processing power of the target and makes the services provided by the target unavailable. The distributed nature of the services makes it impractical. Also, the mobile ad hoc networks are more vulnerable than the wired networks. The interference-prone radio channel and the limited battery power is the reason behind the vulnerability.

4.1.3. *Wormhole Attack*

Wormhole attacks are severe threats to MANET routing protocols. When the attacker records packet at a place, and redirects them to another location, routing is disrupted. This occurs because of the redirection. Such mishaps are nomenclatured as WORMHOLE ATTACKS.

4.1.4. *Modification*

It affects the integrity of data. The attacker alters the packet.

4.1.5. *Spoofing*

Spoofing occurs when a malicious node pretends as some other node. It does so to alter the vision of the network topology that an innocent node can gather[10]. Spoofing is also called the man in the middle. The attacker achieves this, by showing it's IP as the IP of the node it wants to act as.

4.1.6. *Fabrication*

Attacks performed by generating false routing information, are fabrication. These are difficult to identify since they come as valid routing constructs, especially in the case of erroneous . They claim that a neighbour can no longer be contacted.

4.1.7. *Sybil Attack*

When one node impersonates a group of nodes, it is known as Sybil attack. This is a complex attack as a node depends on many intermediate nodes for communication, and so there are redundant algorithms to ensure the delivery of data. However, if a single malicious node is able to represent many nodes, it becomes simpler for the attacker. Now, the destination nodes cannot interpret the change in packets. Fake recommendations about the integrity of a certain party can also be delivered, thus attracting more traffic to it.

4.2. *Passive*

In passive attacks, the routing protocol is not disturbed. Valuable information like node hierarchy and network topology is obtained. The attacker's goal is to obtain information that is being transmitted. Passive attacks are very difficult to identify as they do not involve any modification of data. The following are passive attacks.

4.2.1. *Eaves Dropping*

The goal of eavesdropping is to obtain some confidential information during communication. The confidential information may include the location, public key, private key or even passwords of the nodes. It is crucial that such data are kept hidden from unauthorized people.

4.2.2. *Traffic Analysis*

In this attack, the attacker scrutinizes the traffic, determine the location, discover communicating hosts, detect the frequency and length of message being exchanged. These information are used to predict the nature of communication. All incoming and outgoing traffic of network is not altered.

4.2.3. *Monitoring*

The nodes are monitored. The packet transactions and other activities of the node are verified and audited.

5. SECURITY MECHANISMS IN MOBILE AD HOC NETWORKS

In General there are two kinds of security techniques in MANET, which are intrusion detection and secure routing techniques.

5.1. *Intrusion Detection*

An Intrusion Detection System (IDS) is an indispensable part of a security system and is mainly introduced to detect possible violations of the security policy by monitoring system activities and responding to those that are apparently intrusive. If an attack is detected once in the network, a response is initiated to avoid or curtail the damage to the system [5].

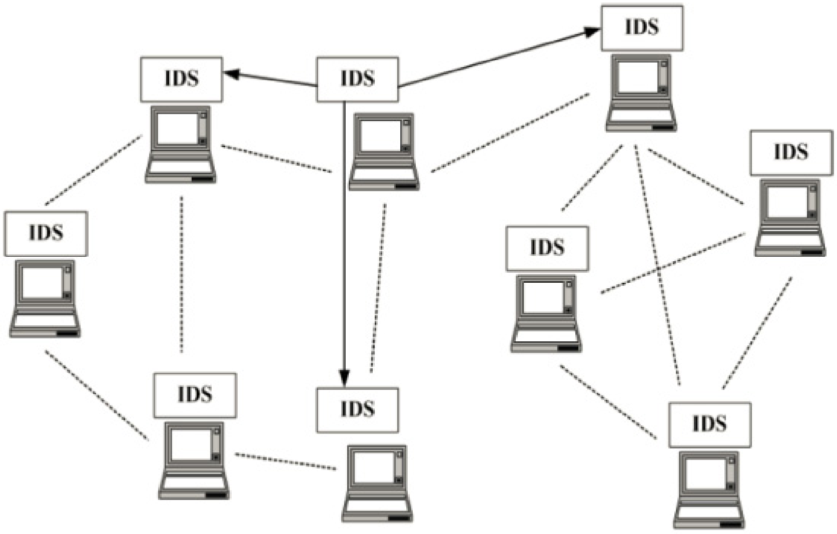

Figure 1: A Simple IDS Architecture for Mobile Ad hoc Network

5.1.1. *Misuse-based Intrusion Detection*

Misuse-Based IDSs detection attack signatures with current system activities[5]. They are generally preferred by commercial IDSs since they are efficient and have a low false positive rate. The main drawback is that it cannot detect new attacks. There is a need for frequent updating of database, since the system is only as strong as its signature database.

5.1.2. *Anomaly-based intrusion Detection*

It detects intrusions as anomalies, i.e. deviations from the normal behavior patterns. The normal activities which are detected as anomalies by IDS can be high in anomaly-based detection and also it is capable of detecting unknown attacks.

5.1.3. *Specification-based Intrusion Detection*

In this part, intrusions are identified as runtime infringement of the terms of routing protocols. They are generally used to detect modification and forge attacks. However, this technique cannot detect attacks that do not violate protocol specifications directly.

5.2. *Secure Routing*

There are numerous kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more sophisticated and harder to detect than others, such as Wormhole attacks and Rush attacks.

5.2.1. *Watchdog and Pathrater*

Watchdog and Pathrater expands performance of MANET in the presence of misbehaving nodes. Watchdog identifies misbehaviour by storing packets to be forwarded into a buffer and it promiscuously sneaks to decide if the neighbour node forwards the packets without alteration or not. If the packets that are sneaked match with the observing node's buffer, then they are discarded. Whereas packets that reside in the buffer beyond a timeout period without any successful match are marked as having been dropped or altered. The node responsible for forwarding the packet is then noted as being suspicious. If the number of infringement becomes greater than a certain predetermined threshold, the node is marked as being malicious. Information about malicious nodes is passed to the Pathrater component for inclusion in path rating evaluation.

Pathrater on a separate node works to rate all of the well-known nodes in a particular network. Ratings are made, and updated, from a particular node's perspective. Nodes start with an unbiased rating that is altered over the time based on the observed behaviour during packet forwarding. Nodes that are observed by watchdog to have misbehaved are given an immediate rating of -100. It should be differentiated that misbehaviour is detected as packet mishandling/modification, whereas unreliable behaviour is detected as link breaks.

5.2.2. *A Secure Ad hoc Routing Approach using localized Self-healing Communities*

The concept of "self-healing community" is based on the examination that wireless packet forwarding typically depends on more than one immediate neighbour to transmit packets. Community-based security delves into node redundancy at each forwarding step so that the conventional per-node based forwarding scheme is flawlessly converted to a new per-community based forwarding scheme [6]. Since a self-healing community is purposeful only when there is at least one cooperative "good" node in the community.

Several routing techniques help in making secure the ad hoc routing security. Some of them deal with specific attacks that aim to disturb the ad hoc routing services, and provide some solutions to help defend against these attacks whereas other techniques try to provide some effective tools or schemes to protect the ad hoc routing services from all kinds of attacks. Because routing service is one of the most important network services in the mobile ad hoc networks, there may be newly emerging attack types against the ad hoc routing all the time to defend the ad hoc routing service against them.

6. CONCLUSION

Through this paper the researcher has tried to understand what MANETs are, their traits and uses. The various criterion, upon which the safety of the network is evaluated are also realized. Crucially, the various vulnerabilities in MANETs, and also the possible attacks that can occur are studied. The study of the above makes well equipped on the understanding of the possible problems in MANETs. It helps in deciding an effective technique to solve the presented problem. The final study on the security measures, show the possible solutions to all given problems. Moreover, the study of the above would help researchers to understand the underlying methods, the shortcomings of the existing systems, and gives them a clear idea on the direction the research should proceed to develop a better system with enhanced features.

REFERENCES

[1] 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.

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

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

[4] Yau P.-W., Mitchell C.J., “Security Vulnerabilities in Ad Hoc Networks”, In Proc. of the 7th Int. Symp. on Communications Theory and Applications, pp. 99-104, 2003

[5] Jim Parker, Anand Patwardhan, and Anupam Joshi, “Detecting Wireless Misbehavior through Cross-layer Analysis,” in *Proceedings of the IEEE Consumer Communications and Networking Conference Special Sessions (CCNC’2006),* Las Vegas, Nevada, 2006.

[6] 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.

[7] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks”, in *Proceedings of ICNP’02,* 2002

[8] Stajano F., Anderson R., “The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks”, In Proc. of Int. Workshop on Security Protocols, Springer, 1999.

[9] Wu B., Chen J., Wu J., Cardei M., “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, Wireless/Mobile Network Security, Chapter 12, Springer, 2006

[10] Y. Hu, A. Perrig and D. Johnson, Ariadne: A , “Secure On-demand Routing Protocol forAd hoc Networks”, in *Proceedings of ACM, MOBICOM’02,* 2002.