Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Security Threats in Wireless Mesh Networks

G. Satyavathy
Assistant Professor, Computer Science,
Affiliated to Bharathiar University, Tamilnadu, India

S. Ananthi
Research Scholar, Computer Science,
Affiliated to Bharathiar University, Tamilnadu, India

Abstract– Wireless mesh networks (WMN) function as regular wireless networks, but with significant differences. Mesh networks decentralize the infrastructure required to maintain a network by making each node, or computer, pull double-duty as a user and a router of Internet traffic. This way, the network exists as an organic and self-managed entity capable of servicing a varying number of users. This survey paper mentions physical attacks , denial of service and passive monitoring and also describes the countermeasures.

Keywords– Wireless Mesh Networks, Internet Traffic, Physical Attacks, Deniel of service, Passive Monitoring

I. INTRODUCTION

Wireless Mesh Networks (WMNs)[1] are considered as a promising solution for offering low-cost access to broadband services. WMN are summarized by self-organization, selfconfiguration and self-healing to enable flexible integration , quick deployment, easy maintenance, low cost, and it may also be used to improve the performance of multi-hop ad-hoc networks. It explains the security threats and attacks at physical layer and medium access control.[2]

II. OVERVIEW OF MESH NETWORKS

It consists of mesh clients and mesh routers. It is used to improve the flexibility of mesh networking, a mesh router[3] is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. WMNs can be classified depending on the architecture in infrastructure /backbone WMNs, A Survey on Security and Privacy Issues in Wireless Mesh Networks client WMNs and Hybrid WMNs. In infrastructure WMNs mesh clients can join the network only through the mesh routers. In client WMNs mesh nodes constitute the actual network while in Hybrid WMNs mesh client may join the mesh network either by connected to the mesh backbone or among each other.

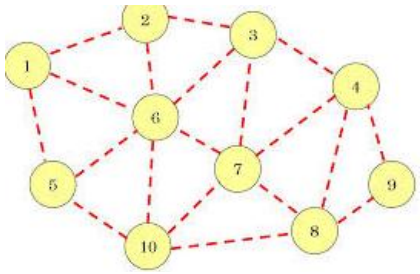

Fig 1: Wireless Mesh Networks

III. SECURITY ISSUES[4]

The key issues are as below:

(i) Availability: Group of nodes in the mesh network infrastructure is suggested in our proposal, where mesh network functionalities are assigned to specific nodes, thus it helps to enhance the network availability.

(ii) Authorization: It is a process in which an entity is issued credentials by the trusted certificate authority. It is generally used to assign different access rights to different level of users.

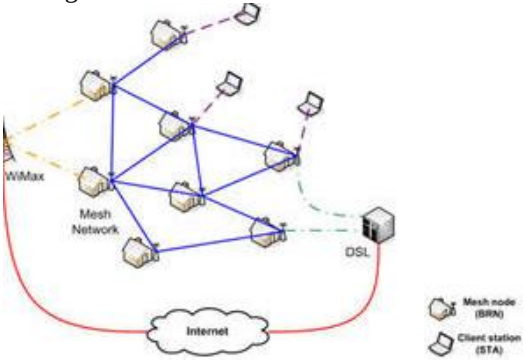

Fig 2 : Security Issues inWMN

(iii) Anonymity: Anonymity means that all the information that can be used to identify the owner or the current user entity should be kept private and not distributed to other communicating parties.

(iv) Confidentiality: It guarantees that the information is only available to those who have been authorized to access it.

IV. SECURITY CHALLENGES AND CONSTRAINTS

A WMN is exposed[5] to the same basic threats common for both wired and wireless networks, therefore the messages in such networks can be intercepted, modified, delayed, replayed, or new messages can be inserted. However, WMNs are more difficult to be fully protected for the following reasons

(i) Multihop Nature: Multihopping delays the detection and treatment of the attacks . Also, since the majority of the existed security schemes are developed for one-hop networks, render them insufficient to protect a WMN from being attacked.

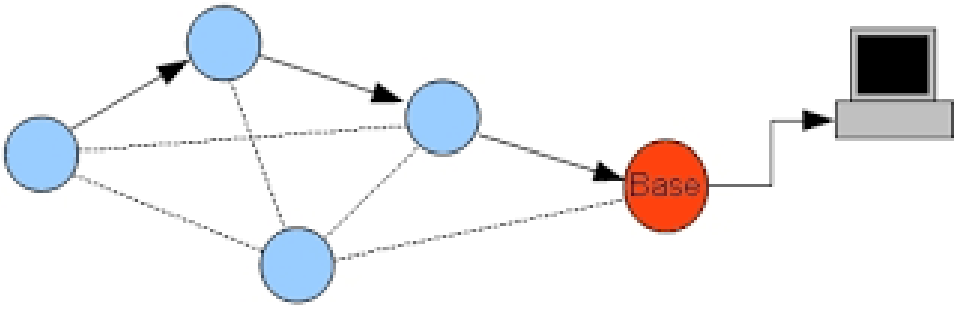

Fig 3: Security challenges using Multihop

(ii) Multitier System security: In such networks security is needed not only between the client nodes, but also between mesh clients and mesh routers, as well as among mesh routers.

V. SECURITY ATTACKS

Security attacks may be classified based on several factors, like the nature, the scope, the behaviour, or the protocol layer the attacker target. Moreover, the attacks can be classified, based on method the attacker use to accomplish their goal, on impersonation, modification, fabrication, replay and Denial of Service (DoS) attacks. In impersonation attacks, an adversary attempts to assume the identity of a legitimate node of the WMN in order to consume its resources or to disrupt the network operation.

1) Security Attacks at the physical layer of WMNs

There are several types of attacks that can affect the physical layer of a WMN. First, since the wireless mesh routers may be installed in external area, an attacker may simply destroy the hardware of such a node. The trivial jamming, periodic jamming, reactive jamming attacks are may be applied in the physical layer. In trivial jamming attack, attacker transmits the noise continuously. In periodic jamming attack (or scrambling attack), an attacker sends a short signal periodically.

2) Security Attacks at the MAC layer of WMNs

Several different attacks are also possible at the MAC layer of the WMNs. These include:

Passive eavesdropping: It can be launched by internal, as well as, external nodes. Due to the WMN‘s broadcast nature of transmission, it is possible for external attackers within the transmission range of the communicating nodes to launch passive eavesdropping. WMNs are also prone to internal eavesdropping by the intermediate hops, whereby a malicious intermediate node may keep the copy of all the data that it forwards without the knowledge of any other nodes in the network

Jamming Attack: At MAC layer jamming attacks[6] are also possible. In this case, the attacker instead of transmitting bits, he/she may transmit regular MAC headers on the transmission channel

Flooding Attack: An attacker sends a lot of MAC control messages to its neighbour nodes.

3) Security Attacks at the Network layer of WMNs

An attacker could also target the network layer of WMNs.

The main control plane attacks are distinguished in:

Rushing Attack: In on-demand routing protocols, the attacker sends a lot of routing request packets across the network in a short interval of time keeping other nodes busy from processing legal routing request packets.

Routing Table Overflow: In this attack[7] the attacker attempts to create routes to non-existent nodes with intention to create enough routes in order to prevent new routes from being created or to overwhelm the protocol implementation.

Location Disclosure: A location disclosure attack reveals information about the location of nodes or about the structure of the network.

Route error injection Attack: During this attack, a malicious node injects forged route error messages to break mesh links and disrupt the routing services.

4) Security Attacks at the Transport Layer

In this layer are flooding and desynchronization, i.e. the disruption of an existing connection. In the flooding attack, a malicious node may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit.

5) Security Attacks at the Application Layer

In WMNNs Application Layer attacks in wireless networks concern viruses, worms, malicious codes, application abuses. Also when data are transmitted unencrypted, they are vulnerable to packet sniffing, as well as, to attacks against applications.

VI. COUNTERMEASURES

The current section discusses several countermeasures for WMNs.

A. Intrusion Prevention Mechanisms[8]

Intrusion prevention mechanisms are considered as the principle line of defense against malicious nodes and include encryption and authentication as well as, secure routing.

B. Secure Routing

Due to open medium, the routing protocols are constantly victims of attacks trying to compromise their capabilities. Therefore the routing protocol used inside a mesh should be secured against attacks. To obtain this goal, researchers proposed either mechanisms to enhance existing routing protocols used for ad-hoc networks or new security protocols that are suitable for WMNs.

C. Intrusion Detection Systems (IDSs)[9]

Since, only the usage of protection and encryption software to protect WMNs are not sufficient and effective, intrusion detection systems are also deployed to provide a second line of defence. Intrusion Detection Systems in wired or wireless networks are used to alert the users about possible attacks, ideally in time to stop the attack or mitigate the damage. They consist of three functions:

1. Event monitoring[10]: The IDS must monitor some type of events and maintain the history of data related to these events.

2. Analysis engine: The IDS must be equipped with an analysis engine that processes the collected data to detect unusual or malicious behaviour.

3. Response: the IDS must generate a response, which is typically an alert to system administrators.

VII. CONCLUSIONS

Wireless Mesh Networks is nowadays a very popular technology for providing IP services due to its fast, easy and inexpensive network deployment. In this paper, we provided a detailed analysis of the fundamental security challenges and constrains of these networks. Furthermore, we classified the possible attacks based on several factors, like the nature, the scope, the behavior or the protocol layer the attacker target. We have also surveyed several defence methods exclusively for WMNs, including intrusion prevention, detection, and response mechanisms.

REFERNCES

[1] S. Seth, and A. Gankotiya, "Denial of Service Attacks and Detection Methods in Wireless Mesh Networks", In the Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (ITC 2010), Koshi, Kerala, 2010 , pp. 238 –240.

[2] Y. Zhang, J. Luo and H. Hu, " Wireless Mesh Networking: Architectures, Protocols and Standards", Auerbach Publications, ISBN: 978-0- 8493-7399-2, 2006.

[3] A. Naveed, S. S. Kanhere, and S. K. Jha, "Attacks and Security Mechanisms Security in Wireless Mesh Networks", Ed (Y. Zhang), Auerbach Publications, ISBN: 978-0-8493-8250-5, 2009.

[4] I. Akyildiz and X. Wang, "Wireless Mesh Networks (Advanced Texts in Communications and Networking", John Wiley & Sons Ltd. ISBN: 978-0-040-03256-5,2009.

[5] J. Sen, "Secure Routing in Wireless Mesh Networks", Wireless Mesh Networks, N. Funabiki (Ed.), InTech, ISBN: 978-953-307-519-8, 2011.

[6] D. Divyaand S. Kumar, "Security Challenges in Multihop Wireless Mesh Networks–A Survey", Information Security and Digital Forensics, D. Weerasinghe (Ed) , Springer Berlin Heidelberg, ISBN: 978-3-642-11530-1, 2010.

[7] H. Redwan and K. Ki-Hyung, "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks", In the Proceedings of the 2008 New Technologies, Mobility and Security Conference (NTMS 2008), Tangier, Morocco, 2008, pp. 1-5.

[8] B. Wu, J. Chen, and J.Wu, A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks Wireless Network Security, Y. Xiao, X. S. Shen, D.-Z. Du (Ed.), Springer, ISBN: 978-0-387-33112-6978-0-387-33112-6, 2007.

[9] D. Bansal, S. Sofat, and A. K. Gankotiya, "Selfish MAC Misbehaviour Detection in Wireless Mesh Networks", In the Proceedings of 2010 International Conference on Advances in Computer Engineering (ACE 2010), Bangalore, Karnataka, India, 2010, pp. 130-133.

[10] H Yang, H Luo, F Ye, S Lu, and L Zhang, "Security in mobile ad hoc networks: challenges and solutions", IEEE Wireless Communications, vol. 11, no. 1, February 2004, pp. 38 – 47.

