Taxonomy of Network Layer Attacks in Wireless Mesh Network

K. Ganesh Reddy and P. Santhi Thilagam

Department of Computer Science and Engineering, NITK Surathkal, India
{guncity11,santhisocrates}@gmail.com

Abstract. Wireless Mesh Networks (WMNs) have emerging application because of its ad-hoc features, high internet bandwidth capability, and interoperable with various networks. However, all features of WMNs vulnerable due to their inadequate security services, and most of the existing techniques protect WMNs only.from single adversary node, but these techniques are failed to protect against multiple colluding attacks, and also have same reputation value for all types of attacks. To overcome these problems for future solutions, we have done clear analytical survey on network layer attacks. Eventually, we have come up with taxonomy of network layer attack.

Keywords: colluding attacks, intrusion detection, wireless mesh, network layer.

1 Introduction

Wireless mesh networks (WMNs) have been emerged as a key technology for providing fast and hassle free services to users and inspiring numerous applications. In recent years, wireless mesh networks have been becoming more popular because of its ubiquitous broadband wireless internet connectivity in a sizable geographic area and cost effective network deployment. WMNs also support features such as dynamic self-organization, self-configuration and self-healing.

Fig. 1 depicts wireless mesh network architecture. Here all wireless radio nodes are connected in mesh to form infrastructure mesh and client mesh in which nodes are ordered hierarchy: gateway, router, and mesh client. WMNs can also interoperate with other wireless networks such as high-speed metropolitan area mobile networks, backhaul connectivity for cellular radio access networks, intelligent transport system, network defense system and citywide surveillance systems.

The study shows that wireless mesh networks are more vulnerable especially in Network layer followed by MAC layer and Physical layer because of open medium, multihop wireless network, heterogeneous networks, dynamic topology and physical threat [6][9][15]. This paper, we classify the network layer attacks and their interdependencies. Network layer attacks are mainly classified into two types: control plane and data plane. Control plane adversaries affect the route discovery and maintenance phase of reactive, proactive, etc. routing protocols.

Here, adversary node creates attacks by itself such as blackhole, rushing attacks, or combine with other adversaries such as wormhole and colluding attacks. Moreover,

D.C. Wyld et al. (Eds.): Advances in Computer Science, Eng. & Appl., AISC 167, pp. 927–935.
springerlink.com

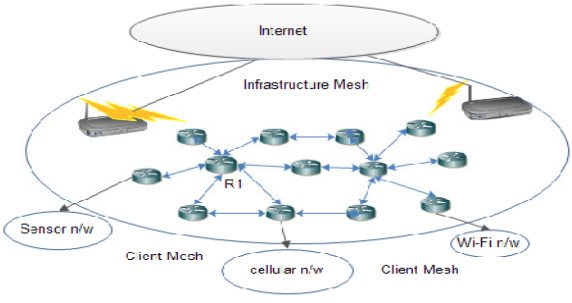

Fig. 1. Wireless Mesh Network Architecture

all the adversaries are internal attackers, and to prevent these attacks existing prevention techniques are ineffective. Other alternative for this problem is Intrusion Detection (ID), many ID techniques have been proposed for single adversary attacks (attack specific) [4][2]. However, very few existing ID techniques are available to protect colluding attacks. However, these solutions are inadequate protect against the all network layer attacks because lack of clear classification of attacks and their interdependencies. Furthermore all these ID techniques follows same reputation value for all type of attacks, it is because lack of available attacks classification. To overcome these problems we have designed taxonomy of network layer attacks, which mainly concentrates on attacks and their interdependencies. In the following, section 2 describes the network layers attacks classification, Section 3 describes conclusion.

2 Network Layer Attacks

WMN lacks robust standard security frameworks, due to this, network layers are more vulnerable to various types attacks. Since WMN supports all wireless networks, it inherits the vulnerability of the protocols supporting that networks. In survey, we found that, there is no in-depth classification of attack on network layers. As a result, existing security solutions are attacks specific, and these solutions cannot detect more than one attack effectively. To overcome these problems, in this section, we have classified all possible attacks on network layers of WMNs.

Fig.2 depicts the taxonomy of network layer attacks. Network layer attacks are classified into two types: Control plane and Data plane attacks. In control plane attacks, adversary intention is to disturb the routing functionalities and/or gain the network traffic of the targeted node. In data plane attacks, adversary (selfish or compromised node) intention is to drop the data packets, injects the false packets, delays the packets etc. In both cases, the adversary may be either internal or external attacker. Internal adversary node is more harmful compare to the external adversary node because it has enough privileges to participate in routing and data forwarding phases. Whereas, external adversary node waste more time to gain the knowledge of target node. We classified the control plane and data plane attacks in the following: