Chapter 4
Securing Wireless Ad Hoc Networks:
State of the Art and Challenges

Victor Pomponiu
University of Torino, Italy

ABSTRACT

The wireless technologies are bringing significant changes to data networking and telecommunication services, making integrated networks a reality. By removing the wires, personal networks, local area networks, mobile radio networks, and cellular systems, offer an entirely distributed mobile computing and communications environment. Due to their unique features such as shared medium, limited resources, and dynamic topology, wireless ad hoc networks are vulnerable to a variety of potential attacks. However, the common security measures employed for wired networks are not enough to protect the nodes of the networks against complex attacks. Therefore, a new line of defense, called intrusion detection, has been added. In this chapter, first we introduce the main wireless technologies along with their characteristics. Then, a description of the attacks that can be mounted on these networks is given. A separate section will review and compare the most recent intrusion detection techniques for wireless ad hoc networks. Finally, based on the current state of the art, the conclusions, and major challenges are discussed.

INTRODUCTION

In the last decades, the widespread diffusion of wireless networking has bought crucial changes in modern communication technologies. Wireless networking enables devices with wireless capabilities to communicate without being connected physically to a network. In general, wireless networks aim to increase the user mobility by extending the wired local area networks (LANs).

A *wireless ad hoc network* is a new *decentralized* wireless networking paradigm. It consist of a set of fixed/mobile modes that rely on each other in order to perform the main networking operations

DOI: 10.4018/978-1-4666-4707-7.ch004

(i.e. routing, packet delivery and route discovery) without the aid of any infrastructure (Giordano, 2002). The changing topology and decentralized management, together with pervasive deployment of various services are the main characteristics of the wireless ad hoc networks (Raghavendra, Sivalingam, & Znati, 2004; Stojmenovic, 2002; Xiao, Chen, & Li, 2010). Further, wireless ad hoc networks can be categorized into *mobile ad hoc networks* (MANETs) which are autonomous systems of mobile nodes, *wireless mesh networks* (WMNs) that are multihop systems in which nodes, organized in a mesh topology and assisted by a wireless card, and *wireless sensor networks* (WSNs). In Figure 1 the main wireless and wired networks types are shown.

Although military and security-strategic operations remain the primary application for ad hoc networks, recently the commercial interest in this type of networks began to grow. For instance, the use of ad hoc networks for emergency missions in case of natural disasters, for law enforcement procedures, for community networking and interaction, for monitoring the weather conditions and for public healthcare (Baronti et al., 2007; Milenkovic, Otto, & Jovanov, 2004; Neves, Stachyra, & Rodrigues, 2008; Perrig et al., 2002).

As the deployment of ad hoc networks spread to numerous application environments, security remains one of the main challenges of these networks. The attacks that can target an ad hoc network can be broadly classified into *passive attacks* and *active attacks*. Passive attacks collect sensitive information from the network without jeopardizing the communications among the nodes. Instead, an active attack interferes and changes the functionality of the network by blocking, forging and modifying the information flow (Wu, Chen, Wu, & Cardei, 2006). Depending on the source of origin, the security attacks could also be split into *outside attacks* and *inside attacks* (i.e. attacks originating from the compromised nodes).

The classical security mechanism employed to protect the wired networks is not suitable for ad hoc networks in many cases. The unique feature that creates these security issues is the lack of centralization, i.e. each node is responsible for routing, packet forwarding and network administration (Molva, & Michiardi, 2003). Contrast to the special-purpose nodes of the wired network (i.e., routers, switches and getaways), the nodes of an ad hoc network are not reliable for accomplishing the critical network operations. Furthermore, authentication and encryption, which both rely on

Figure 1. Different networks types. The intrusion detection techniques for the networks in bold face are the focus of this study.