Chapter XXXIII
Cutting the Gordian Knot:
Intrusion Detection Systems in Ad Hoc Networks

John Felix Charles Joseph
Nanyang Technological University, Singapore

Amitabha Das
Nanyang Technological University, Singapore

Boon-Chong Seet
Auckland Univerisity of Technology, New Zealand

Bu-Sung Lee
Nanyang Technological University, Singapore

ABSTRACT

Intrusion detection in ad hoc networks is a challenge because of the inherent characteristics of these networks, such as, the absence of centralized nodes, the lack of infrastructure, and so forth. Furthermore, in addition to application-based attacks, ad hoc networks are prone to attacks targeting routing protocols. Issues in intrusion detection in ad hoc networks are addressed by numerous research proposals in literature. In this chapter, we first enumerate the properties of ad hoc networks which hinder intrusion detection systems. After that, significant intrusion detection system (IDS) architectures and methodologies proposed in the literature are elucidated. Strengths and weaknesses of these works are studied and are explained. Finally, the future directions which will lead to the successful deployment of intrusion detection in ad hoc networks are discussed.

INTRODUCTION

Wireless ad hoc networks have attracted extensive attention among researchers in recent years. As the research activities matured, it has been widely realized that security in such networks is a major issue, and an extremely challenging one. The challenge arises mainly from the inherent

characteristics of ad hoc networks. Chief among the characteristics, which affect the design of an effective security framework for such networks, are the highly distributed, decentralized, and dynamic natures of ad hoc networks. These properties, coupled with the lack of infrastructure in ad hoc networks, introduce some unprecedented issues, which are absent and never been explored in conventional networks.

A typical security system consists of two major components. The first is the intrusion prevention mechanism that aims to control access to the system and relies mainly on cryptographic techniques. The second one is the intrusion detection system that tries to detect if the prevention mechanism has been compromised by intruders, and if so, come up with an appropriate response to combat such intrusions. The intrusion detection system (IDS) thus forms the second line of defense (Nadkarni & Mishra, 2003).

Cryptographic techniques rely on secure key management and key distribution which require supporting infrastructure. The lack of infrastructure makes it extremely difficult to implement cryptographic access control mechanisms in ad hoc networks. This makes intrusion detection all the more important for such networks. However, it turns out that the inherent characteristics of ad hoc networks render conventional IDS unsuitable for such networks. This has spawned the research in ad hoc IDS design (Brutch & Ko, 2003).

This chapter illustrates the difficulties in providing an efficient intrusion detection system for ad hoc networks. In doing so, it discusses in detail interesting ad hoc IDS models proposed in literature. The strengths and weaknesses of these models are explained and promising future directions for cutting the Gordian knot of ad hoc IDS are discussed.

BACKGROUND

Although various analyses on intrusion detection mechanisms can be seen in the literature, only few qualify as significant. Mishra, Nadkarni, and Patcha (2004) give a detailed overview of various ad hoc IDS architectures and methodologies. They offer an extensive analysis and understanding of IDS in ad hoc networks. A comprehensive comparison between various proposed intrusion detection systems for ad hoc networks are discussed. Selected architectures and detection strategies explained by Mishra et al., which were found significant, are detailed in this writing.

Zhang, Huang, and Lee (2005) propose an evaluation environment for MANET (mobile ad hoc network) intrusion detection systems. They emulated routing attacks and evaluated application-based intrusion detection architectures over it. The work introduces a novel concept of evaluating ad hoc IDS models using known attacks. Routing attack libraries are used, which exhibit attack scenarios over the IDS model under-evaluation. The IDS models are evaluated for operational cost and effectiveness. Detection accuracy and false alarms are the primary evaluation parameters for assessing of the IDS model, in terms of detection effectiveness. The work is significant in providing a test-bed for ad hoc IDS models. Similarly, Little (2005) proposes a test-bed called TeaLab for ad hoc IDS design.

Concurrent to simulation-based ad hoc test-beds, Yang and Baras (2003) mathematically analyze vulnerabilities in ad hoc networks. The authors provide a great deal of understanding to the attack possibilities in ad hoc domain. Mathematical methods find attacks exhaustively. In this theoretical analysis all possible attacks are hypothesized. This comprehensive vulnerability analysis aids the design of an effective ad hoc IDS design.

CHARACTERISTICS OF AD HOC NETWORKS

Ad hoc networks differ from native wired/wireless networks in various aspects. These unique characteristics of ad hoc networks render typical security systems unsuitable (Awerbuch, Curtmola, Holmer, Rubens, & Nita-Rotaru, 2005; Papadimitratos & Haas, 2002). The fundamental concept of ad hoc networks is to have seamless connectivity without infrastructure or centralized control. The lack of