Chapter 60
Hybrid Intrusion Detection Framework for Ad Hoc Networks

Abdelaziz Amara Korba
Badji Mokhtar-Annaba University, Algeria

Mehdi Nafaa
Badji Mokhtar-Annaba University, Algeria

Salim Ghanemi
Badji Mokhtar-Annaba University, Algeria

ABSTRACT

In this paper, a cluster-based hybrid security framework called HSFA for ad hoc networks is proposed and evaluated. The proposed security framework combines both specification and anomaly detection techniques to efficiently detect and prevent wide range of routing attacks. In the proposed hierarchical architecture, cluster nodes run a host specification-based intrusion detection system to detect specification violations attacks such as fabrication, replay, etc. While the cluster heads run an anomaly-based intrusion detection system to detect wormhole and rushing attacks. The proposed specification-based detection approach relies on a set of specifications automatically generated, while anomaly-detection uses statistical techniques. The proposed security framework provides an adaptive response against attacks to prevent damage to the network. The security framework is evaluated by simulation in presence of malicious nodes that can launch different attacks. Simulation results show that the proposed hybrid security framework performs significantly better than other existing mechanisms.

INTRODUCTION

Wireless multi-hop ad hoc networks are becoming very attractive and widely deployed in many kinds of communication and networking applications. However, distributed and collaborative routing in such networks makes them vulnerable to various security attacks. Intrusion detection and prevention

DOI: 10.4018/978-1-5225-9866-4.ch060

mechanisms can detect malicious activities performed by external or internal attackers, by monitoring and analyzing network activities. The intrusion detection mechanisms can be classified into three main classes based on the employed detection technique. The first technique is anomaly-based intrusion detection which defines the normal behavior of the system using classification and statistical methods. It detects any anomalous observed activity that deviates significantly from the normal behavior as intrusion. The advantage of this technique is its ability to detect unknown attacks, however it generates high false positives rate, and induces high computational cost. Signature-based detection compares current system activities with signatures or patterns of known attacks. It is reliable and has low false positive rate, however it cannot detect new attacks. Specification-based detection specifies the normal behavior using a set of rules and constraints, and detects intrusions as runtime violations of the specification. It generates low false positive rate and can detect unknown attacks, however defining specification is a time-consuming process.

Most of the existing protection mechanisms in the literature detect one or particular type of attack and thus provide a partial protection. The majority of the proposed intrusion detection mechanisms employ anomaly-based detection because it can detect unknown attacks. However, anomaly-based detection can be inefficient against certain type of attacks such as specification violation and generate high false positive alarms. On the other hand, specification-based detection mechanisms can only detect specification violation attacks. We think using one detection technique limits the range of detected attacks and detection performance. Although intrusion prevention and intrusion response are normally part of the intrusion detection mechanism, they have received less attention than detection function in the literature. While host-based intrusion detection system cannot detect distributed attacks, purely distributed and cooperative architecture can generate significant extra overhead. These limits and deficiencies in the existing protection mechanisms are the main motivation behind this work.

In this paper, first we discuss routing attacks both specification violation and fast-forwarding (wormhole and rushing), and classify them into basic and compound attacks. Then we propose a hierarchical hybrid security framework which combines anomaly-based and specification-based detection techniques and takes advantage of both techniques. Cluster heads run anomaly-based IDS to detect fast-forwarding attacks using a statistical method which is more adapted to the nature of these attacks. Cluster nodes run a specification-based IDS to detect specification violation attacks using an automatically generated model which exemplifies the normal operation of the routing protocol. We propose an adaptive intrusion response against malicious nodes. Simulation results show that our intrusion detection and prevention framework outperforms other schemes proposed in the literature in terms of number of detected attacks, detection rate and false positive rate. The main contributions in this paper are as follows:

1. We design a novel anomaly-based intrusion detection system that uses statistical techniques to detect wormhole and rushing attacks and identifies malicious node by monitoring traffic model.
2. Specification-based detection depends on manual extraction of the specification model, which makes it error prone and time-consuming. To overcome these deficiencies, we propose a new approach to automatic extraction of specification model of routing protocol, which is expressed through the use of a finite state machine (FSM).
3. We design a novel specification-based intrusion detection system which detects and prevents specification violation attacks.
4. We propose an adaptive intrusion response scheme to punish malicious nodes.