Chapter 13

A Secure Routing Scheme Against Malicious Nodes in Ad Hoc Networks

Abdelaziz Amara Korba
Badji Mokhtar-Annaba University, Algeria

Mohamed Amine Ferrag
Guelma University, Algeria

ABSTRACT

This chapter proposes a new cluster-based secure routing scheme to detect and prevent intrusions in ad hoc networks. The proposed scheme combines both specification and anomaly detection techniques to provide an accurate detection of wide range of routing attacks. The proposed secure scheme provides an adaptive response mechanism to isolate malicious nodes from the network. A key advantage of the proposed secure scheme is its capacity to prevent wormhole and rushing attacks and its real-time detection of both known and unknown attacks which violate specification. The simulation results show that the proposed scheme shows high detection rate and low false positive rate compared to other security mechanisms.

INTRODUCTION

Distributed and collaborative routing in ad hoc networks makes them vulnerable to diverse security attacks. Intrusion detection and prevention systems represent powerful mechanisms to protect network against external and internal malicious activities. Based on the detection technique, there are mainly three classes of intrusion detection system: Knowledge-based intrusion detection (SBID), anomaly-based intrusion detection (ABID); and specification-based intrusion detection (SBID). This paper proposes a secure routing scheme that combines both anomaly-based and specification-based detection techniques, with an adaptive intrusion response. Specification-based technique is used to detect attacks which violate routing protocol specification, anomaly-based technique to detect attacks that violate other layer protocol specification (fast-forwarding attacks). This paper proposes an automatic specification extrac-

DOI: 10.4018/978-1-5225-5736-4.ch013
A Secure Routing Scheme Against Malicious Nodes in Ad Hoc Networks

In order to identify patterns of attacks, IDAR compares logs with a set of predefined signatures, where

BACKGROUND

Different techniques have been used to implement anomaly-based intrusion detection such as those proposed in Mitrokotsa & Dimitrakakis (2013), most of them are based on statistical approaches, and artificial intelligence methods. In Buczak and Guven (2015) the authors surveyed machine learning and data mining methods used for cyber intrusion detection. The paper provided description of the use of different machine learning and data mining techniques in the cyber domain, both for signature-based and anomaly-based intrusion detection. In addition to addressing the complexity of different methods, the paper discussed challenges of using machine learning algorithms for cyber security, and provided some recommendations.

Jabbehdari, Talari, and Modiri (2012) proposed an intrusion detection system based on neural networks to detect DoS attacks in MANETs. Barani and Abadi (2012) proposed an anomaly-based IDS named BeeID which can detect a wide range of attacks using a hybrid approach based on the artificial bee colony (ABC) and negative selection (NS) algorithms. Nadeem and Howarth (2013a) proposed a cluster-based intrusion detection and adaptive response mechanism (IDAR), which is an extension of their previous proposal generalized intrusion detection and prevention mechanism (GIDP) (Nadeem & Howarth, 2013b). IDAR combines signature-based and anomaly-based techniques. In the first phase, a cluster head gathers audit data from network nodes, and then uses collected data to build training profiles. Finally, the testing module is launched periodically to detect possible intrusion, and identify attacks and intruders. The IDS takes action once the attack is occurred, and it is not able to prevent its occurrence. Continuous data gathering, repeated training, attack inference, and knowledge base management are time, bandwidth and resource consuming tasks. A trade-off should be made between workload, classification accuracy, and energy consumption. Furthermore, constructing and adding a rule for the new attacks is prone to generate false attack signatures.

Karri and Santhi Thilagam (2014) proposed a reputation-based cross-layer IDS to detect wormhole attack. The proposed mechanism analyses the behaviors of the routing node in wireless mesh networks to correctly detect wormhole route and isolate wormhole nodes. In the context of smart grid, (Beigi, Jelena, Hamzeh, & Vojislav, 2013) proposed a wormhole detection scheme by using geographical locations of nodes (GPS) to estimate the shortest path length between nodes. The proposed model described the relation between Euclidean distance and the corresponding hop count along the shortest path. Based on the model, the receiver node can estimate the smallest hop count to the sender, and thus detect wormhole nodes in the path.

Alattar and Alattar (2016) proposed IDAR, a signature-based distributed intrusion detection based on OLSR (Clausen & Jacquet, 2003). IDAR extracts evidence from OLSR collected logs, and according to the activity’s suspicion level, it initiates in-depth cooperative investigation to confirm intrusion. In order to identify patterns of attacks, IDAR compares logs with a set of predefined signatures, where
Related Content

Risk Assessment of Incidents Response for Downstate New York Natural Gas Distribution Infrastructure

Pre-Service Language Teachers' Experiences in the Digital Storytelling Process
Melih Derya Gürer (2020). *IT Issues in Higher Education: Emerging Research and Opportunities* (pp. 87-112).
[www.igi-global.com/chapter/pre-service-language-teachers-experiences-in-the-digital-storytelling-process/237666?camid=4v1a](www.igi-global.com/chapter/pre-service-language-teachers-experiences-in-the-digital-storytelling-process/237666?camid=4v1a)

ECFS: An Enterprise-Class Cryptographic File System for Linux
[www.igi-global.com/article/ecfs-enterprise-class-cryptographic-file/68821?camid=4v1a](www.igi-global.com/article/ecfs-enterprise-class-cryptographic-file/68821?camid=4v1a)

A Retrospective on the Development of Web Service Specifications
[www.igi-global.com/chapter/retrospective-development-web-service-specifications/28513?camid=4v1a](www.igi-global.com/chapter/retrospective-development-web-service-specifications/28513?camid=4v1a)