Journal of Computer and System Sciences 80 (2014) 554–570

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Algorithms for a distributed IDS in MANETs ☆, ☆☆

P.M. Mafra [a,b,*], J.S. Fraga [a], A.O. Santin [c]

[a] Automation and Systems Department, PGEAS, UFSC, Caixa Postal 476, CEP 88040-900, Florianopolis, SC, Brazil
[b] Federal Institute of Santa Catarina, Sao Jose, SC, Brazil
[c] Pontifical Catholic University of Parana, Curitiba, PR, Brazil

ARTICLE INFO

Article history:
Received 30 November 2012
Received in revised form 30 April 2013
Accepted 14 June 2013
Available online 9 July 2013

Keywords:
Intrusion detection system
Mobile ad hoc networks
Distributed systems
Fault tolerance
Network security

ABSTRACT

This paper presents a set of distributed algorithms that support an Intrusion Detection System (IDS) model for Mobile Ad hoc NETworks (MANETs). The development of mobile networks has implicated the need of new IDS models in order to deal with new security issues in these communication environments. More conventional models have difficulties to deal with malicious components in MANETs. In this paper, we describe the proposed IDS model, focusing on distributed algorithms and their computational costs. The proposal employs fault tolerance techniques and cryptographic mechanisms to detect and deal with malicious or faulty nodes. The model is analyzed along with related works. Unlike studies in the references, the proposed IDS model admits intrusions and malice in their own algorithms. In this paper, we also present test results obtained with an implementation of the proposed model.

1. Introduction

The last decade has witnessed a great evolution in communication technologies and models that promote mobility and self-organization. Mobile Ad hoc Networks (MANETs) are an example of self-organized networks where there are no concentrator units (gateways) and the environment is highly dynamic with nodes joining and leaving at any time [2]. However, such networks are susceptible to a great variety of attacks. The challenge that arises is to maintain the MANET free from the activity of malicious or faulty nodes. In the face of the difficulty of avoiding the effects of malicious activities, mechanisms are necessary to at least minimize such effects. Intrusion detection systems (IDSs) can be used as one of these mechanisms [3]. However, many well-known proposals and experiences of distributed IDSs do not tolerate the presence of malicious or faulty nodes among its nodes. Most of the studies about this issue in the literature do not employ the use of cryptographic mechanisms in communications of IDS nodes, even if this communication depends on the cooperation of nodes that do not belong to the system. The key question in those IDSs is to ensure that applications in MANET environments can always evolve despite of failures, attacks by malicious entities or their own mobility.

Works in this area deal mainly with problems applied to routing protocols in MANETs [4] and some works focus on problems of malicious behavior [3–6]. These works are limited to monitoring the communications in MANETs and to propose IDS models, usually having components which centralize its decisions or information. Moreover, in the literature, the IDSs developed for MANETs usually do not have mechanisms to protect their own information and do not tolerate intrusions into its various components.

☆ This research has been supported by The National Council for Scientific and Technological Development (CNPq), Grants 310671/2012-4 and 307588/2010-6. Paulo Manoel Mafra wishes to thank the Coordination for the Improvement of Higher Level Personnel (CAPES) for the scholarship granting.
☆☆ An earlier version of this paper was published in [1].
* Corresponding author at: Automation and Systems Department, PGEAS, UFSC, Caixa Postal 476, CEP 88040-900, Florianopolis, SC, Brazil.
E-mail addresses: mafra@das.ufsc.br (P.M. Mafra), fraga@das.ufsc.br (J.S. Fraga), santin@ppgia.pucpr.br (A.O. Santin).

0022-0000/$ – see front matter
http://dx.doi.org/10.1016/j.jcss.2013.06.011

The communication among entities in MANETs can be monitored by distributed components of an IDS in order to detect faulty or malicious behavior, and to improve security and reliability of such dynamic environments. In this paper we propose a secure and fully distributed IDS model for MANETs. The algorithms presented in this paper define an IDS with functions performed by sets of components (fully distributed executions) and with mechanisms and techniques for preventing and tolerating malicious activities of their own components.

The proposed system is able to deal with various faulty or malicious nodes and mobility without there being interference in the IDS's expected correctness. The proposed IDS, unlike other works, uses cryptographic mechanisms to guarantee the messages authentication between its elements. Moreover, the proposal is able to identify a large number of different attacks or variations of known attacks. The employment of distributed systems and dependability concepts in the IDS design allows modeling, within certain limits, a system less susceptible to restrictions.

This paper is organized as follows. Section 2 describes the related works and defines some parameters and attributes for being used in qualitative analyses. Section 3 introduces the organization of our distributed IDS, defining its components and their roles in the proposed model. We also describe some assumptions of our model and system dynamics. In Section 4 we present the algorithmic base to support the secure IDS. In Section 5 we describe asymptotic costs of the algorithms and results of performed tests in a simulator. Finally, in Section 6, we present our conclusions.

2. Related work

During the last decade many intrusion detection systems were proposed. In 2000, Marti et al. [7] proposed "watchdog and pathrater" mechanisms. The goal of such study was to detect nodes that do not forward packets. Excluding such nodes from routing caches will reduce their effects on MANET routing protocols. Changes were proposed to the Dynamic Source Routing (DSR) protocol [8] for including the watchdog and pathrater mechanisms. The behavior of nodes, in forwarding packets, is observed through the number of dropped packets. If a threshold value for any node is reached, the node is marked as malicious.

In 2003, Zhang, Lee and Huang [9] proposed a distributed and cooperative IDS architecture for MANETs. In that architecture, each node has an IDS agent participating in intrusion detection and response activities. These IDS agents act in a cooperative way by composing a collection of IDSs. The architecture in [9] is merely conceptual and was not implemented.

In [3] Kachirski and Guha proposed an IDS for MANETs using, in each system node, sensor agents that assume functions of data monitoring, decision making and also responding to the malicious activities. The network is divided into clusters in that work. A cluster head is defined in each cluster to route data between clusters. The cluster head is selected based on distances among nodes in the same cluster as well as on the number of neighbors of each node. Monitoring data collected by all sensor agents are merged for detecting intrusions.

Also in 2003, an IDS based on non-overlapping zones named ZBIDS was proposed by Sun, Wu and Pooch [10]. That proposition deals with the problem of cooperation among nodes where the network's nodes are grouped into zones. In ZBIDS, some nodes act as gateways to inter-zone communications. Each node must know its physical location in order to be included into a pre-established zone. For that, the authors suggested that each node must have a GPS locator. The intrusion detection method is based on Markov Chains. Study cases of ZBIDS were simulated using the network simulator GloMoSim [11].

In 2006, another IDS based on clusters was proposed by Ahmed and his colleagues for collaborative detections of intrusions [4]. Cluster compositions are formed and maintained in fixed periods of time. Each cluster has a leader which monitors all the traffic inside its cluster. This leader is also responsible for inter-cluster communications. Message exchanges in the IDS are not protected by the use of cryptography, thus making information and decisions of the IDS easily corrupted under various types of security attacks.

In [12], another model of collaborative IDS was introduced by Razak and Furnell. In the proposal, the node which detects suspect activity requests opinions from its neighbors concerning the detected activity. After analyzing each neighbor's vote, the node makes a decision and informs it to the participating nodes.

Another study introducing an IDS model was presented by Sterne and Lawler [13]. The model is also based on a node hierarchy where the lowest level collects the data and the higher levels correlate the collected data. However, that study goes further than previous cited works. The proposed model allows the detection of several malicious nodes in the IDS's own composition. However, the malicious nodes may only belong to the lower levels of the proposed hierarchy.

In the work of Rajaram and Palaniswami [14], it was described a proposition of an IDS for MANETs which includes a trust-based security protocol, taking into account a MAC-layer mechanism. The protocol provides packet authentication and confidentiality in both routing and link layers of MANETs. In the protocol's first phase, a trust-based scheme for packet forwarding is used to detect and isolate malicious nodes. It uses trust values to favor packet forwarding. When a trust counter value falls below a reliable threshold, the corresponding intermediate node is marked as malicious. In the second phase of the protocol, a link-layer security scheme was developed using the authentication and encryption CBC-X mode to provide security in the IDS messages exchange.

Another distributed cooperative IDS for MANETs was proposed by [15]. That IDS relies on local and global analysis. Each node has a local IDS engine, which runs the network-based IDS *Snort* that monitors the neighbor nodes network activity. Once a node detects a suspicious activity, it starts a distributed IDS algorithm that receives all relevant data about the intrusion detection. In this algorithm, the data received from the IDS engine as well as any other IDS alert message