Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 1203 – 1208

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

A Distributed Self-Adaptive Intrusion Detection System for Mobile Ad-hoc Networks using Tamper Evident Mobile Agents

Deepa Krishnan[a,]*

[a]*Pillai Institute of Information Technology Media Studies and Research Centre,New Panvel,Mumbai,410206,India*

Abstract

This paper brings forth a distributed self adaptive intrusion detection system (IDS) based on programmable mobile agents which can act as a key line of defense against major security attacks. The proposed intrusion detection model is organized as a combination of the two trends in IDS; the rule based and the behavior based scheme. Also this model draws out the merits of both the host based and networks based IDSs and deploy them wisely considering the critical features of MANETs. In contrast to many proposed and implemented IDSs, this is an efficient framework conscious of the inherent constraints of MANETS and are self adaptive in nature. In addition to this, the use of light weight mobile agents provide a low overhead mechanism which in turn is well suited to MANET characteristics. Through this paper, an attempt to improvise the mobile agents is done by making it tamper evident which is very essential as the agents can be compromised and thereby turning all the efforts of the IDS futile.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: Mobile Ad-hoc Networks, adaptability, mobile agents, Intrusion detection system, tamper evident;

1. Introduction

In recent decades, MANETs have been widely used in many critical applications and with wide spread usage security became a challenging problem for this prominent technology. This is mainly due to the design properties of ad hoc networks like peer-to-peer multi-hop infrastructure-less network architecture, shared wireless medium,

* Corresponding author. Tel.: +91977-342-3043; fax: +0-222-748-3208.
E-mail address: dkrishnan@mes.ac.in

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.01.034

stringent power and bandwidth constraints and above all, the highly dynamic network topology with frequently changing channel access and routing decisions. Mobile ad hoc networks face additional security problems compared to the traditional infrastructure based wired networks. Thus, efficient security mechanisms are the need of the hour. However, we should remember the fact that most of the security techniques designed and tested for wired networks seem to be unsuitable for ad hoc networks. Hence, when designing any security technique, the key features of MANETS should be well considered. This paper concentrates on Intrusion Detection System as it is always a major line of defense against attacks and a widely accepted proactive defense strategy.

This proposed scheme is designed considering dynamic nature of MANETs and its various associated constraints. It provides a light weight, low overhead Intrusion Detection Scheme which is based on programmable mobile agents. This direction draws benefits from both the behavior based and rule based schemes. The behavior based approach is in turn coupled with efficient fuzzy logic training schemes to significantly reduce the false positives and increase detection rates. The highlight of this work is that it ensures the security of its agents by making it tamper evident. The beauty and effectiveness of this approach is that the entire IDS scheme revolves around the use of programmed and dynamic mobile agents to achieve all the functionalities.

2. Background Study

2.1. Study of Various IDS Schemes

One commonly used IDS classification scheme is the behavior based detection which is built on a long term monitoring and classification of what is expected/normal or abnormal. This scheme is very challenging to implement due to the dynamic nature resulting in random communication patterns. Another approach is the rule based model which requires maintenance of an extensive database of all attack patterns and needs to be periodically updated at each node. This approach cannot be relied alone as it incurs more computational cost and may not be effective in detecting new attacks.

Another direction in the IDS classification is the Distributed Vs Centralized schemes. A distributed IDS scheme uses cooperative detection strategies to determine an attack whereas in Centralized approach decision is taken unilaterally. There is one more classification related to the distribution of functionality as flat and hierarchical approach. In the flat architecture every node in the network shares same responsibilities and tasks in intrusion detection and decision making whereas in the hierarchical architecture, nodes have varying functionalities with one root node making control decisions.

2.2. Related Works

Several efforts has been made in the design of Intrusion detection systems for MANETs, however most of them couldn't bring out an efficient and reliable scheme which covers all aspects of MANET security. One of the pioneering works in this field is[1] by Zhang and Lee in which they have described a distributed and cooperative intrusion detection system for MANETs. In this model, they have used a flat architecture and the IDS agents deployed in the mobile nodes are given equal importance. However, each of these look for malicious activities in their respective nodes and it is only in instances of inconclusive evidences that intrusion detection is performed using cooperative voting method. Intrusion detection is done in a distributed and cooperative manner, however at the core it functions in a flat architecture.

Another related architecture is suggested by Smith in his mobile-agent based IDS architecture[2] for wireless ad-hoc networks. The work by Smith is also in a similar direction as that of the previous one wherein a flat architecture and distributed co-operative manner for intrusion detection is used. The difference between this model and the one explained in [1] is that it uses agents that are static and follow RPC schemes for communication whereas Smith make use of mobile agents. The potential benefits of using mobile agents like reduced network latency and communication overhead and improved scalability are very well explained in [3, 4 ,5].