# Chapter 25
# Agents for Intrusion Detection in MANET: A Survey and Analysis

**Leila Mechtri**
*Badji Mokhtar University, Algeria*

**Fatiha Djemili Tolba**
*Badji Mokhtar University, Algeria*

**Salim Ghanemi**
*Badji Mokhtar University, Algeria*

## ABSTRACT

*Mobile Ad-hoc NETworks (MANETs) are believed to be highly vulnerable to security threats due to the numerous constraints they present such as: the absence of a fixed infrastructure, the dynamic topology change, their dependence on cooperative communication, the unreliability of wireless links and most importantly the absence of a clear line of defense. Since intrusion detection and agent technology proved to offer several potential advantages, there has been a great tendency for using agents to build optimal, adaptive and comprehensive intrusion detection systems to fit MANET security requirements. This chapter presents a survey and analysis of the work that has been recently done for the deployment of agent technology in the area of MANET intrusion detection. In particular, recent advances in that field in terms of existing frameworks, architectures and implementations as well as a discussion of the obtained advantages in addition to the potentially introduced vulnerabilities are presented.*

## INTRODUCTION

Over the past years, Mobile Ad-hoc NETworks (MANETs) have raised several challenging security-related issues. The inherent nature of the wireless medium together with the distributive structure of these networks makes them susceptible to a wide variety of security threats ranging from passive eavesdropping to active interference. Moreover, these networks are highly resource constrained in terms of

DOI: 10.4018/978-1-5225-9866-4.ch025

network topology, memory and computational abilities, which complicated the design and deployment of security solutions. Considering these issues, securing MANETs by means of traditional security mechanisms such as firewalls and authentication is deemed unsatisfactory.

For that, there is always a need for intrusion detection systems (IDSs) to guarantee an acceptable security level. In MANET, IDSs are, generally, classified into four main classes (architectures), namely, stand-alone IDSs, distributed and cooperative IDSs, hierarchical IDSs and agent-based IDSs. Contrary to stand-alone IDSs, where the detection process is performed on each node, and there is no cooperation or data exchange between the network nodes, distributed and cooperative IDSs suggest that every node in the MANET must participate cooperatively in intrusion detection and response. Hierarchical IDSs, on the other hand, are the most suitable for multi-layered networks where the network is divided into clusters. The main idea behind this architecture is that instead of performing host-based intrusion detection at each node, a cluster head is selected to collect security-related information from nodes in a cluster and determines if an intrusion has occurred. The last architecture of MANET IDSs, denoted agent-based IDS architecture, is based on the distribution of the intrusion detection tasks amongst a number of agents.

It is worth noting that contrary to former IDS architectures (stand-alone, distributed and cooperative, and hierarchical) which were excessively used for the development of MANET IDSs, the studies that approach agent-based IDSs were quite few in the early years of IDS deployment in MANET. This is mainly due to: (i) the additional complexity involved in developing agent-based IDSs especially as this technology is known for introducing new challenges with respect to security mainly when dealing with mobile agents and (ii) the lack of experience in formulating agent-based solutions to applications. However, as they, recently, proved several advantages, agents are gaining great attention especially for their suitability for the building of distributed applications. This is what encourages many researchers to explore more possibilities for the application of agents in the context of MANET intrusion detection. This paper presents an up-to-date survey of the state of the art in the area of MANET intrusion detection with a great emphasis on the application of agent technology in this context.

This paper is organized as follows: section 2 outlines the basic features of IDSs, agents and agent-based technologies. Then, section 3 focuses on the recent advances, in terms of the proposed frameworks, architectures and implementations, for the application of agent technology to MANET intrusion detection. Section 4 presents and discusses the drawn conclusions about agent deployment in MANET intrusion detection, with respect to the studied frameworks. Finally, some concluding remarks are given in section 5.

## BACKGROUND

In this section we introduce some concepts and terminology related to the field of agent-based intrusion detection.

### Intrusion Detection

Intrusion detection is the process of monitoring and analyzing events of computer systems or networks in order to uncover any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource (Hung-Jen, Chun-Hung, Ying-Chih, & Kuang-Yuan, 2013).