Modeling an Intrusion Detection System Based on Adaptive Immunology

Vishwa Alaparthy, Electrical Engineering, University of South Florida, Tampa, USA
Salvatore D. Morgera, Electrical Engineering, University of South Florida, Tampa, USA

ABSTRACT

Network security has always has been an area of priority and extensive research. Recent years have seen a considerable growth in experimenting with biologically inspired techniques. This is a consequence of the authors increased understanding of living systems and the application of that understanding to machines and software. The mounting complexity of telecommunications networks and the need for increasing levels of security have been the driving factors. The human body can act as a great role model for its unique abilities in protecting itself from external entities owing to its diverse complexities. Many abnormalities in the human body are similar to that of the attacks in wireless sensor networks (WSN). This article presents the basic ideas that can help modelling a system to counter the attacks on a WSN by monitoring parameters such as energy, frequency of data transfer, data sent and received. This is implemented by exploiting an immune concept called danger theory, which aggregates the anomalies based on the weights of the anomalous parameters. The objective is to design a cooperative intrusion detection system (IDS) based on danger theory.

KEYWORDS

Danger Theory, Immune System, Intrusion Detection, Network Security, WSN
1. INTRODUCTION

Successful behavioral and communication stratagems of a Bio network can serve as an inspiration to model and manage a wireless network. This can be due to the fact that the sophistication provided by a bio network is very intriguing and intuitive. Also, the robustness provided by a bio network is noteworthy and truly unique. This coupled with the need for lower power dissipation and sub optimal energies in a wireless sensor network make human body a great source of inspiration. The large volume of research in Bio Inspired Intrusion detection systems is also due to the inadequacy of successful conventional techniques. Providing security to a wireless network has always been an overwhelming task. Although various levels of security have been provided to a system or a node, the adversaries tend to find a way to break through these layers. The affected node can divulge some information or sometimes turn into an attacker. The operational strategies of a WSN such as a multi hop approach, also considerably weakens the security measures of the system. Due to such numerous challenging aspects of designing a security system, a self-adaptive, self-healing model is essential. Due to the most complex nature of human body and its ability to protect itself from external pathogens, it is considered a perfect role-model. Many successful techniques have been put forward over the years related to the security of wireless networks. Design of inexpensive cryptographic techniques has been the crux of most of those solutions. Installing an Intrusion Detection system or a firewall can be some other alternative solutions. Design of an Intrusion Detection system using Bio Inspired approaches is also not uncommon. Many Anomaly-based detection algorithms [Kim, Hakju &Kwanjo, 2005; Hosseinpur, Amouli & Hämäläinen, 2014] have been proposed to detect unknown-attacks. Artificial Immune System (AIS) (Hofmeyr & Forrest, 2000) and Ant Clustering Algorithm (ACA) (Li & Xia, 2015) are members of bio-inspired machine learning algorithms used to implement Anomaly-based detection. AIS is inspired by human immune system and has capability to differentiate normal and abnormal states. ACA is inspired by the movements of ants and makes clusters by using simple movements of a number of artificial ants. (Forrest, Perelson, Allen & Cheruluri, 1994) proposed a negative selection mechanism for anomaly based detection which attempts to identify the self and non-self antigens/nodes creating artificial peptides can be a way of differentiating self and non-self nodes. (Greensmith, Aickelin & Cayzer) proposed an anomaly detection algorithm for computer networks based on danger theory by using Dendritic cells, which emits danger signals. This paper presents a model, which attempts to build an IDS specifically for WSN based on immune system inspired techniques. A number of quantified signals are generated based on the anomalies originated in various features of a WSN which are aggregated and an intrusion is detected. Unlike the previous approaches, which use a single resource to look for an anomaly, this approach unifies various parameters such as energy, data transmitted and frequency of data transfer. More information regarding these parameters is given in the later parts of this paper. Section 2 gives a brief
RFID Technology in Business and Valuation Methods
www.igi-global.com/chapter/rfid-technology-in-business-and-valuation-methods/115147?camid=4v1a

A Data Gathering Algorithm Based on Energy-Aware Connected Dominating Sets to Minimize Energy Consumption and Maximize Node Lifetime in Wireless Sensor Networks
www.igi-global.com/article/data-gathering-algorithm-based-energy/46964?camid=4v1a