Application of Artificial Immune Systems for the Creation of IoT Intrusion Detection Systems[1]

Marin Emilov Pamukov
Telecommunications Faculty
Technical University - Sofia
Sofia, Bulgaria
marinpamukov@gmail.com

***Abstract* - The advances made in the field of IoT in recent years implore us to take a closer look at the security challenges it presents. Due to its ubiquitous nature and high heterogeneity of the connected devices and communication protocols a novel approach must be taken. This papers aim is to make a brief review of the work done in the areas of Negative Selection and Danger Theory and to do a comparative analysis of the available solutions. Furthermore, the most prominent characteristic an artificial immune system must attain in order to conform to the unique security requirements put forward by the IoT are identified.**

Index Terms - IoT, Artificial Immune System, Intrusion Detection Systems, Security, IDS

I. Introduction

A major challenge in computer security is the self/nonself differentiation. Traditionally blacklisting is used to solve this issue, by creating lists of allowed actors and operations. In IoT networks the issue [1] is further exacerbated due to their architecture. As a first step in tackling this issue is the creation of a common Framework. Most of the proposed frameworks emphasize the use of Intrusion Detection Systems (IDSs) as a cornerstone for creating secure IoT systems [2] [3].

This makes us consider the use of Artificial Immune Systems (AIS) for the purpose of creating a comprehensive Intrusion Detection System (IDS). The Human Immune System can detect and organize a defense against previously unknown pathogens. An Intrusion Detection System that mimics those properties would have the advantages of high false positive tolerance, unsupervised learning and self-adaptation.

During the last few decades AIS have been a topic of interest for many scientists, with the goal of solving complex engineering and computational problems. Several types of artificial immune systems have been the main object of investigation: The Negative Selection Algorithm (NSA) and Danger Theory (DT).

II. Negative Selection Based Algorithms

The Early work of Forrest et al. [4] deserves mentioning. They propose the use of randomly generated detectors. After the set is generated it goes through a maturation period, during which it is exposed to the "self" set. The self-reactive detectors are removed and replaced with new ones. This simple aproach demonstrated a 100% detection rate under certain conditions.

In [5], [6] Homfrey and Forrest propose a Network IDS called LISYS. The system implements an AIS architecture called ARTIS [7]. LISYS uses a NSA to generate a binary detectors set. The NS algorithm is also used for determining the activation threshold, life span, decay rate and creating memory detectors. To monitor the network traffic LISYS examines the TCP connections and extracts the source and destination IP address and the TCP port. This information is used to classify the packets as either self or non-self. In LISYS an RCBM rule is used. If a detector is similar to an antigen in a predetermined consecutive number of bits alarm is raised. If a detector produces a sufficient amount of alarms, it is promoted to a memory detector and becomes a part of the permanent antigen set of the AIS. Memory detectors have a lower activation threshold than normal ones. LISYS uses costimulation from an administrator to determine if an alarm represents real threat to the system. Balthrop et al. [8], [9] analyse the adaptive characteristics and attempt to quantify the performance of the individual underlying algorithms of LISYS. The results demonstrate that the individual algorithms of the system are capable of solving diferent machine learning problems. The use of activation thresholds, sensitivity levels, r-chunks and permutation masking improves the levels of false positives. Furthermore, the co-stimulation and the implementation of memory lymphocytes improves the on-line and one-class learning capabilities of the system.

In [10] Harmer et al. expanded on an earlier version of CVIS [11] , with the goal of implementing the system for network intrusion detection. They named their IDS CDIS. It utilizes the concepts of lifespan of the detectors, activation threshold and co-stimulation. The system monitors numerous features of the TCP, UDP and ICMP protocols in order to detect intrusions. CDIS chooses randomly one of the protocols and a set of features. It then randomly generates values for these features. It adopts the concept of affinity maturation for the purpose of further optimizing the antibody set generation. The results show that CDIS is able to reliably detect intrusions under certain conditions. As a downside of the system the authors

[1] This work was supported by the Program for Financing PhD Students Research,
Technical University – Sofia, Bulgaria,
Contract №162ПД0028-07,
Research topic: "Developing AIS based Intrusion Detection System for the IoT ";