Multiple Negative Selection Algorithm: Improving Detection Error Rates in IoT Intrusion Detection Systems[1]

MSc. Eng. M. E. Pamukov
Telecommunications Faculty, Technical University - Sofia
Sofia, Bulgaria
marinpamukov@gmail.com

PhD. Prof. Eng. V. K. Poulkov
Telecommunications Faculty, Technical University - Sofia
Sofia, Bulgaria
vkp@tu-sofia.bg

***Abstract*—The creation of intrusion detection systems for IoT scenarios presents various challenges. One of them being the need for an implementation of unsupervised learning and decision making in the detection syste[1]m. The algorithm presented in this paper is capable of definitively identifying a large percentage of possible intrusions as true or false without the need of operator input. Our proposal is based on the Negative Selection algorithm and the co-stimulation principles of Immunology. It uses a two-tiered negative selection process to implement a co-stimulation approach aimed at decreasing the number of detection errors without the need of an operator input.**

***Index Terms*— Computational Immunology, Negative Selection, NS, Artificial Immune Systems, AIS, Security, IDS, Intrusion Detection System, IoT, Internet of Things, Co-stimulation**

I. Introduction

The concept of Internet of things (IoT) is based on the idea of connecting billions upon billions of heterogeneous devices and networks, thus presenting a myriad of technical difficulties and challenges, the most prominent one being security [1]. As a first step in tackling the security 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].

In this paper we examine the Artificial Immune System (AIS) based IDSs that use negative selection and analyze their applicability to IoT. Furthermore, we isolate some shortcomings of the available designs and propose as a possible solution, a modification of the Negative Selection Algorithm (NSA). We call this algorithm Multiple NSA (MNSA). Its major advantage is the identification of a large percentage of possible intrusions as true or false without the need of operator input. Our proposal is based on NSA and the co-stimulation principle of Immunology. It uses a two-tiered negative selection to implement a co-stimulation, aimed at lowering the detection errors without the need for human input. Similar approach is applied in [4] where an e-mail spam classification system is proposed. It uses two detector sets to classify an e-mail as either spam or not.

Further, the paper is organized as follows: Section II provides an overview on the work done in creating IDSs based on Immunological Algorithms (IA). Emphasis is put on NSA, as the simplest IA applicable to IDS creation. We also outline what we perceive as the major issue, hampering wider use of the NS algorithm in IDSs. Section III presents the MNSA along with the applicable detector generation algorithm. Section IV contains the simulation parameters and results, along with short comments regarding the different simulation scenarios. Section V concludes the paper presenting summary of the results and future research issues.

II. Overview

The NSA tries to mimic the maturation of naive immune cells in the Thymus of vertebrates, called clonal deletion. During the clonal deletion process, naive T-lymphocytes are presented with *self*-antigens. The Lymphocytes that demonstrate a high affinity towards the *self* cells undergo a process of apoptosis and are removed from the set [5]. The ability of the NS algorithm for unsupervised learning makes it a viable option for the creation of intrusion detection systems. This feature is especially valuable when dealing with IoT network security. Much work has been done in the area with Forrest et al. [5], being among the first to explore the application of NS for intrusion detection. They propose the use of randomly generated detectors. After a set is generated, it goes through a maturation period during which it is exposed to the *self* set.

[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 ”;