Negative Selection and Neural Network based Algorithm for Intrusion Detection in IoT

Marin E. Pamukov, Vladimir K. Poulkov, and Vasil A. Shterev
Telecommunications Faculty
Technical University – Sofia
Sofia, Bulgaria

***Abstract*—Internet of Things expands the boundaries of the Internet to encompass many devices with constraint computational and power capabilities. This limits the implementation of security techniques such as Intrusion Detection Systems. In this paper, we propose a novel classification algorithm specifically designed for Internet of Things Intrusion Detection Systems. Our solution consists of two distinct layers. First, we employ a Negative Selection algorithm for creating a training set based only on the knowledge of the normal network behavior. Based on this data we train a simple Neural Network that is used to do the actual classification. This multilayer approach allows to distance the training complexity from the computationally and power constrained IoT devices. Furthermore, the addition of Negative Selection layer allows us to train a Neural Network only based on the self/normal behavior of the network, without the need for nonself/attack data. We call this algorithm Negative Selection Neural Network (NSNN). We test the algorithm against the KDD NSL dataset. The test results lead to the conclusion that the proposed algorithm is capable of functioning as network intrusion detection classifier.**

***Keywords*—Neural Networks, Negative Selection, Intrusion Detection System;**

I. Introduction

The number of connected devices is ever increasing, thus the risk to their security. Considering the extent to which most organizations are dependent on fast transfer of large amounts of data, the issue of information security extends well beyond the information itself. Unauthorized access to our data compromises not only our privacy but our liberty as well. In order for the Internet of Things (IoT) concept to gain wider acceptance, several issues must be resolved, security and privacy being the most important.

To better understand and combat the risks that information security, we use the following definition of intrusions:" any set of actions that attempt to compromise the security objectives". Halme and Buer [1] have identified Intrusion Detection Systems (IDS) as one of six anti intrusion systems namely prevention, preemption, deterrence, deflection, detection, and countermeasures. Of these, the self-nonself classification plays a crucial role in all modern security systems. The important role IDSs play in securing a network is of interest to many researchers working in the area of IoT is discussed in [2], [3]. In the context of IoT an IDS faces the following limitations [4]:

- Lack of standardization in many regards (communicational protocols, hardware, provided services, etc.).
- Lack of physical control of the overall IoT environment. The huge amount of installed devices makes it unfeasible to try to physically secure them.
- Many of the IoT devices have limited computational resources.

Based on those limitations we propose the following short list of requirements any IoT IDS must attain:

- Distributed architecture.
- Self-organization capability.
- Low computational complexity.

This paper aims at proposing a solution capable of meeting the abovementioned requirements. The focus is on creating a simple yet powerful algorithm for IoT network based IDS that is:

- Lightweight enough as to be applicable to a wide range of IoT use cases.
- Be capable of detecting previously unknown intrusion vectors.
- Provide acceptable detection rate (F1 score greater than 0.7).

The rest of this paper is structured as follows. In the next section, we make a short overview of IDS, Neural Networks (NN) and Negative Selection Algorithms (NSAs). In section III, we describe the proposed algorithm and provide the pseudocode for the different layers. In section IV we illustrate the simulation setup we designed to test the proposed algorithm's performance. In section V, we present the simulation results and in the final section VI we conclude the paper and outline areas of future work.

This paper was supported by research project DN 07/22/2016 of the Bulgarian Research Fund of the Ministry of Education.