Expert Systems With Applications 60 (2016) 311–320

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Short communication

An efficient proactive artificial immune system based anomaly detection and prevention system

Praneet Saurabh*, Bhupendra Verma

Department of Computer Science and Engineering, Technocrats Institute of Technology, Bhopal, MP 462021, India

ARTICLE INFO

Article history:
Received 18 November 2014
Revised 23 March 2016
Accepted 24 March 2016
Available online 30 March 2016

Keywords:
Security
Anomaly
Self-tuning
Detector power
Agents
Biological Immune System
Artificial Immune System

ABSTRACT

Artificial Immune System (AIS) is inspired from Biological Immune System (BIS) and demonstrates a lot of interesting facets and intelligence that include self-learning, self adaption, self regulatory, distributed with self/non-self detection capabilities. Due to these astonishing qualities AIS are predominantly used in anomaly detection where anomalies are treated as non-self that needs to be detected. Therefore, AIS appears appropriate for development of a proactive system to identify and prevent novel and unseen anomalies. This paper presents "An Efficient Proactive Artificial Immune System based Anomaly Detection and Prevention System (EPAADPS)" which embodies immune attributes to distinguish self and non-self in quest to identify and prevent novel, unseen anomalies. Negative Selection Algorithm (NSA) is a key AIS concept and is used for anomaly detection in various publications. Despite its relative success, detector selection and thereafter anomaly detection demands a more effective algorithm. This paper put forwards concept of self-tuning of detectors and detector power in NSA with the intension to make a detector evolve and facilitate better and correct self and non-self coverage. Thereafter, agents accompanying detectors collaborate and communicate between themselves to proactively discover correct anomalies and then take appropriate preventive measures. The performance of EPAADPS is contrasted with closely related state of art RNS algorithm using real valued representation and Euclidean distance. Experimental results revels promising EPAADPS performance which very comfortably outperforms the RNS. Furthermore, these results also demonstrate that EPAADPS shows remarkable resilience and intelligence in detecting novel unseen anomalies and with preventive measures to overcome the threat perception.

1. Introduction

This decade has witnessed tremendous growth of personal computer and different computing devices. Proliferation of internet with these computing devices brought ease and handiness to almost all the verticals of life. Though this exposure brings a lot of convenience but at the same instance it also introduces security vulnerabilities. Moreover, pervasiveness of internet, availability and access of attack knowledge and methods have contributed in sharp rise of attacks. It is constantly evolving and today's threat landscape cannot be compared to the scenario of previous years (Liu, 2014). Attacks of yesterday were naive, like brute force for password breaking and denial of services. Moreover, it has now transformed to social engineering and devastating worms, tomorrow it might develop in self replicating worms and rootkits because nobody knows what is there in store for future. As a consequence, basic attacks of yesterday that have caused containable damage have given way to modern organized cybercrime operations that are swift, sophisticated and more lethal.

Biological Immune System (BIS) is a complicated yet specific network constituted of different specialized cells, tissues, organs and chemicals with a purpose to apprehend and eliminate any foreign invader and strange elements in the body (Castro & Timmis, 2003). Artificial Immune System (AIS) is a computational intelligent model inspired by the principles and processes of the BIS (Dasgupta & Forrest, 1999, Chap. 14). AIS covers vast area of research and over last few years has attracted attention of researchers due to its appealing features in computational intelligence approach (Jungwon & Bentley, 1999). AIS entices researchers with its attractive qualities which are of self-configuration, self-learning, self-adaptation and distributed coordinating. Above all, it can successfully differentiate between self and non-self (Aickelin, Greensmith, & Twycross, 2004). Due to these qualities AIS is extensively used in anomaly detection (Castro & Timmis, 2003), pattern recognition (Dasgupta, 1999), learning and optimization (Forrest & Hofmeyr, 1999). From the research viewpoint qualities of AIS are

* Corresponding author. Tel.: +91 9329648253.
E-mail address: praneetsaurabh@gmail.com, bkverma3@gmail.com (B. Verma).

http://dx.doi.org/10.1016/j.eswa.2016.03.042
0957-4174/

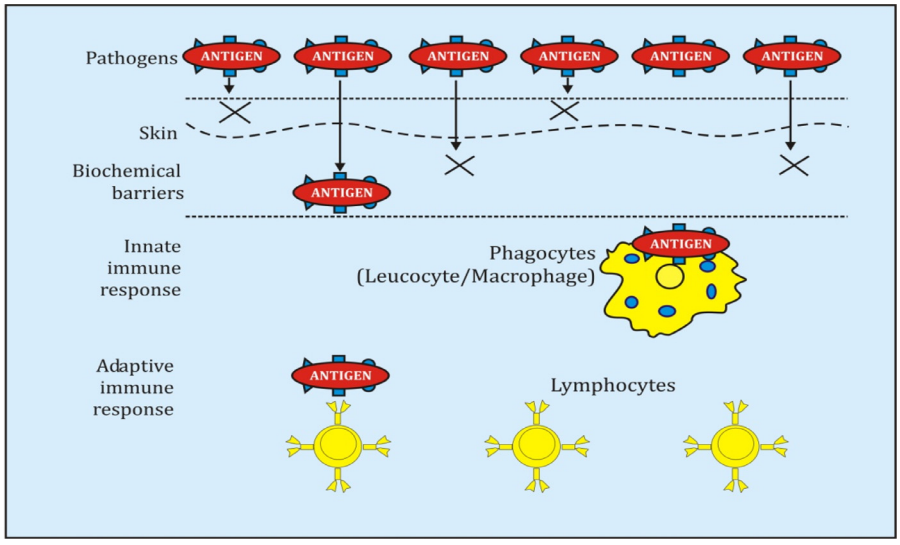

Fig. 1. Multi-layer structure of the Biological Immune System.

the same that are required for a proactive anomaly detection and prevention system. This paper presents An Efficient Proactive Artificial Immune System based Anomaly Detection and Prevention System (EPAADPS) which embodies immune attributes to identify and prevent novel and unseen anomalies. Below are the research objectives of this paper.

(i) To perform a relevant study of existing security solutions inspired and based on AIS.
(ii) To develop a co-operative mechanism for correct decision making in case of attack and thereafter to lower false positives.
(iii) To develop an AIS inspired proactive anomaly detection and prevention system.

Section 2 of this paper covers related work with the viewpoint of AIS and agents in the canvas of anomaly detection and computer security. Section 3 details the proposed EPAADPS. Critical evaluation of experimental results of EPAADPS with closely related state of art RNS is covered in Section 4 followed by discussion in Section 5 and conclusion in Section 6.

2. Related work

Nature of threat and its impact have changed over the years (Sundram, 1996). Various techniques and tools are developed to overcome ever growing threat perception (Zafar, Naheed, Ahmad, & Anwar, 2008). Most of the currently available approaches are based on collecting, analyzing and extracting evidences after an attack which leads to slow reaction time in giving appropriate response to the escalating number of new attacks (Schultz, 2002). Lack of adaptability and self learning capabilities further complicate the problems. These systems work on the convention of collecting, analyzing and extracting evidences after attacks which leads to slow reaction time in giving appropriate response to the escalating number of new attacks (Liu, 2014). Lack of self-learning and self-adapting abilities further escalates failure in detection and prevention of unknown attacks (Napoles, Grau, Falcon, Bello, & Vanhoof, 2016). Moreover, non-availability of abnormal samples at the training stage results in limited performance. These factors contribute in failure in detection of unknown and new attacks despite growth of various computer security arsenal and awareness all these years, but threat perception has neither been eliminated nor mitigated.

Biological Immune System (BIS) in Fig. 1 is a successful multi-layer classification system which makes a distinction between self and non-self. Furthermore, it recognizes “good” self and “not good” non-self (Forrest & Beauchemin, 2007). BIS is constituted by central lymphoid which generates and matures immune cells. Bone marrow constantly produces lymphocytes that mature in thymus. Thymus releases only the matured and beneficial T-cells to the blood stream and discards the remaining ones. These matured cells behave like detectors, identify invading antigens and thereafter take suitable and appropriate measures (Jungwon & Bentley 1999).

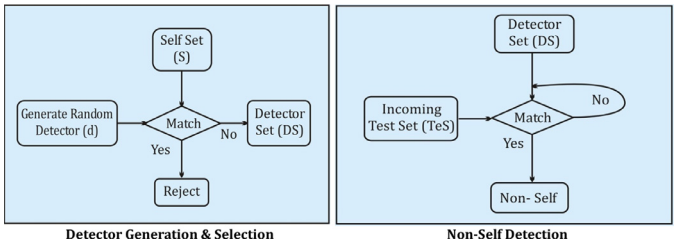

Fig. 2. Negative Selection Algorithm (NSA).

AIS are adaptive computational frameworks driven by the concepts of BIS. AIS has become a new research hotspot due to its appealing features like self-configuration, self-learning, self-adaptation, and distributed coordinating in computational intelligence approach (Nguyen, Nguyen, Mai, & Le, 2014). AIS also successfully demonstrates its ability to distinguish between self and non-self. Various new AIS models in recent years have been proposed to solve different problems from the domain of computer security, data mining, clustering data analysis and classification (Askar et al., 2015; Dasgupta & Forrest, 1999, Chap. 14).

Negative Selection Algorithm (NSA), is one of the most popular AIS models that has grabbed the eyeballs of researchers. Forrest et al. proposed NSA, based on the principles of self/non-self discrimination in the immune system illustrated in Fig. 2 (Forrest, Perelson, Allen, & Cherukuri, 1994). It drew motivation from the fact that negative selection of T cells in the thymus and worked around the immune system’s philosophy to identify unknown antigens/non-self, while not reacting to self-cells. It builds a self profile by recognizing only normal network patterns as self while other patterns as non-self. This built profile very easily detects non-self patterns and marked them as non-self/anomalous. If any sample matches any self-sample then it is removed so that it does not become a detector. Those patterns who fail to match self pattern becomes