A New Model for Dynamic Intrusion Detection

Tao Li[1], Xiaojie Liu[1], and Hongbin Li[2]

[1] Department of Computer Science,
Sichuan University, Chengdu 610065, China
litao@scu.edu.cn
[2] Department of Electrical and Computer Engineering,
Stevens Institute of Technology,Hoboken, NJ07030, USA
hli@stevens.edu

Abstract. Building on the concepts and the formal definitions of self, nonself, antigen, and detector introduced in the research of network intrusion detection, the dynamic evolution models and the corresponding recursive equations of self, antigen, immune-tolerance, lifecycle of mature detectors, and immune memory are presented. Following that, an immune-based model, referred to as AIBM, for dynamic intrusion detection is developed. Simulation results show that the proposed model has several desirable features including self-learning, self-adaption and diversity, thus providing a effective solution for network intrusion detection.

1 Introduction

The problems found in a computer security system [1] are quite similar to those encountered in a Biological Immune System (BIS) [2]. Both systems have to keep stability in a changing environment. Due to numerous desirable characteristics, such as diversity, self-tolerance, immune-memory, distributed and parallel management, self-organization, self-learning, self-adaptation, and robustness, BIS has attracted many researchers' attentions in recent years [3-5]. With the concepts of immunology introduced into many research fields, exciting results have been obtained, especially in the research of network intrusion detection system (NIDS) [2-22].

The negative selection algorithm [8], proposed by Forrest et al. in 1994, has greatly promoted the research of computer immune system (CIS). Hofmeyr and Forrest proposed a general framework for CIS, called ARTIS [9-11], where the concepts and mechanisms of BIS, including self, nonself, self tolerance, immune cell (detectors), memory cell (memory detectors), and costimulation were well simulated. The CISs are mainly derived from ARTIS [2]. For example, Dasgupta and Harmer built an agent-based CIS framework [12-13] upon ARTIS to monitor the network activities.

However, there are two major defects in the present CISs: One is that the self set is very large in size. As the cost for mature detector training is exponentially related to the size of self set [14], the efficiency of the traditional CIS models is very low.

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 72–84, 2005.

The other deficiency is that the definitions of self (normal network behaviors) and nonself (abnormal network behaviors) allow little change after they have been defined in many immune-based models or methods for NIDS [3-14]. In fact, it is very difficult to use fixed definition for self and nonself in most practical applications, since the roles of self and nonself may exchange at times (e.g., the legal network behaviors today may be dangerous tomorrow). Therefore, it is necessary to update the definitions of self and nonself from time to time. The dynamic clonal selection algorithm (DynamiCS) [15] attempted to solve this problem. In DynamiCS, the self elements used in the self tolerance for immature detectors are the survived antigens (those antigens are taken as self elements since they passed the detection) in each detection step, reducing the training cost of the immature detectors. However, as the whole self set in the system is roughly replaced by the survived antigens in each step, too much useful self information is lost, resulting in a high error rate, then, having limited applications.

In addition, the absence of rigorous quantitative descriptions in most presented CIS models results in the randomicity of CIS implementation; therefore, it is not convenient to put these models into practical applications. In this paper, we first present the dynamic evolution models and the corresponding recursive equations of self, antigen, immune-tolerance, lifecycle of mature detectors, and immune memory. Then, we develop a new immune-based model, which is called AIBM, for dynamic intrusion detection. Similar to DynamiCS, AIBM uses a very small dynamic self set during the self tolerance for immature detectors, resulting in a high efficiency in generating new mature detectors. However, different from DynamiCS, the definition of self and nonself in AIBM is dynamic. As time goes on, AIBM can add new self elements into, or eliminate the mutated ones from the self set, resulting in the dynamic evolution of self set, mature and memory detectors, having a lower error rate than traditional CIS models. Our experimental results show that AIBM is an effective solution for network intrusion detection.

The rest of the paper is organized as follows. In Section 2, we establish an immune-based mathematical model for dynamic intrusion detection. In Section 3, simulations and experimental results are provided. Finally, Sections 4 contains our summary and conclusions.

2 Proposed Theoretical Models

Antigens ($Ag, Ag \subset D, D = \{0,1\}^l$) in our approach are fixed-length binary strings extracted from the Internet Protocol (IP) packets transferred in the network. An antigen consists of the source and destination IP addresses, port number, protocol type, IP flags, IP overall packet length, TCP/UDP/ICMP fields, etc., having the characteristics of network activity. And the process of extracting the features of an IP packet to form an antigen is also called the antigen presentation. The structure of an antibody is the same as that of an antigen. Nonself patterns ($Nonself$) represent IP packets from a computer network attack, while self patterns ($Self$) are normal sanctioned network service transactions and nonmalicious background clutter, such that $Self \cup Nonself = Ag$