Extended Thymus Action for Reducing False Positives in AIS based Network Intrusion Detection Systems

M. Zubair Shafiq, Mehrin Kiani, Bisma Hashmi and Muddassar Farooq
College of Electrical & Mechanical Engineering
National University of Sciences & Technology
Rawalpindi, Pakistan
zubairshafiq@ieee.org, {kiani013,b.hashmi}@gmail.com, muddassar.farooq@udo.edu

ABSTRACT
One of the major problems faced by anomaly based Net-
work Intrusion Detection (NID) systems is the high num-
ber of false positives. False positives refer to the false de-
tection of normal behavior as malicious behavior. Artificial Immune Systems (AISs) also fall under the category of anomaly based-NID systems. AIS presented in this paper is as a victim-end filter, consisting of detectors distributed on the network, which distinguishes normal traffic from mal-
cious traffic. In this work, we focus on TCP-SYN flood based Distributed Denial of Services (DDoS) attacks. Light Weight Intrusion Detection System (LISYS) provides the basic framework for AIS based NID systems. AISs normally utilize the negative selection algorithm in thymus action to tolerize the detectors to normal traffic so they may not de-
tect normal traffic as malicious traffic. We propose and implement ‘extended thymus action’ model to improve this characteristic of AIS. Results verify that our model signif-
ically reduces false positives which is a major concern in anomaly-based NID systems.

Categories and Subject Descriptors
D.0 [Software]: GENERAL

General Terms
Experimentation, Performance, Security

Keywords
Artificial Immune System, Network Intrusion Detection

1. INTRODUCTION
NID systems can be classified into two major categories namely signature-based NID systems and anomaly-based NID systems. Signature-based NID systems extract signature from traffic and match it to the stored signatures from a pre-existing library. Anomaly-based NID systems store information about normal behavior and detect deviation from this normal behavior. This allows anomaly-based NID sys-
tems to detect such innovative attacks whose signatures are not stored in the library. But major problem with such sys-
tems is high number of false positives (false alarms).

2. ARCHITECTURE AND RESULTS
Hofmeyr and Forrest proposed a basic architecture (known as LISYS) to cater for TCP-SYN flood based attacks in [1]. We propose an extension to basic thymus action model which is responsible for tuning of detectors so they may not detect normal traffic as malicious traffic. In extended thy-

Figure 1: Extended Thymus Action

We compared our approach of extended thymus action to simple thymus action in a well known network simulator OMNeT++. The comparison was done under different at-
tack scenarios with varying degree of malicious activity. The results obtained through extensive experiments clearly demon-
strate that the proposed model achieves lower number of false positives in different attack scenarios as compared to the system not utilizing our model.

3. REFERENCES