UAEU

جامعة الإمارات العربية المتحدة
United Arab Emirates University

The College of Graduate Studies and the College of Information Technology Cordially Invite You to a

Master Thesis Defense

Entitled

A DENDRITIC CELL ALGORITHM BASED APPROACH FOR MALICIOUS TCP PORT SCANNING DETECTION

By

Nuha Yousef Al Masalmeh

Faculty Advisor

Prof. Zouheir Trabelsi, Department of Information Systems and Security

College of Information Technology

Date & Venue

10:00 AM

Tuesday, 16 April 2019

Room E1-1036, IT Building

Abstract

The proliferation of cyber-attacks is accompanied by an urgent need to develop sophisticated detection tools. Some of these tools are based on algorithms inspired from the Human Immune System (HIS). The Dendritic Cell Algorithm (DCA) is one of such HIS inspired methods, which is based on the Danger theory model.

In this thesis, two types of DCA algorithm are identified, namely the deterministic and classical DCA in order to improve the algorithm's applicability and performance to detect Denial of Service (DoS) attack, namely the TCP port scanning. This algorithm consists of components based on the behavior of Human dendritic cell, which involves four categories of the input signals.

The ultimate goal of this research is to describe the DCA algorithm, implement both types of DCA using Java language and test these implementations by data collected from a real TCP port scan experiment. Three scenarios are conducted to perform this experiment attack, normal and mix scenario. The results show that the DCA can be applied to detect anomalous port scans. The research also compares between the performance of the two DCA in detecting the malicious process.

Keywords: Artificial immune systems, dendritic cell algorithm, denial of service, intrusion detection, port scanning.