TABLE OF CONTENTS

LIST OF ABBREVIATION I
LIST OF FIGURES III
LIST OF TABLES V
LIST OF PUBLICATIONS VII
PREFACE VIII

CHAPTER 1 – INTRODUCTION 1

1.1 OVERVIEW 1
1.2 SECURITY 3
1.2.1 THREATS 6
1.2.2 ATTACKERS 7
1.2.3 SECURITY POLICY AND MECHANISM 8
1.3 EVOLUTIONARY SYSTEMS 9
1.3.1 THE GENOTYPE AND THE PHENOTYPE 10
1.3.2 ARTIFICIAL EVOLUTION 10
1.3.3 TYPES OF EVOLUTIONARY ALGORITHMS 12
1.4 NATURAL IMMUNE SYSTEM 13
1.5 ARTIFICIAL IMMUNE SYSTEM 13
1.5.1 NEGATIVE SELECTION ALGORITHM 15
1.5.2 CLONAL SELECTION ALGORITHM 16
1.5.3 SELF AND NON-SELF 17
1.6 GENETIC ALGORITHMS 18
1.7 ARTIFICIAL NEURAL NETWORKS 19
1.8 Decision Tree Learning 22
1.9 MACHINE LEARNING 24
1.10 ORGANIZATION OF THE THESIS 26

CHAPTER 2 – LITERATURE SURVEY 29

2.1 OVERVIEW 29
2.2 THE HUMAN IMMUNE SYSTEM 31
2.2.1 TYPES OF IMMUNITY 32
2.2.2 ACQUIRED IMMUNITY 32
2.3 COMPUTER IMMUNOLOGY 33
2.4 ARTIFICIAL IMMUNE SYSTEM 35
# Chapter 5 - Immune-Neuro Approach for System Security

5.1 Introduction 93  
5.2 Proposed Methodology 95  
  5.2.1 Range of Parameters 95  
  5.2.2 Range for Learning 95  
  5.2.3 Training Examples 98  
5.3 Neural Network Learning 98  
  5.3.1 Implementation of Gradient-Descent Algorithm 99  
  5.3.2 Range for Learning and Preprocessing for Backpropagation Algorithm 103  
  5.3.3 Implementation of Backpropagation Algorithm 108  
5.4 Experimental Results and Comparisons 114  
5.5 Summary 120

# Chapter 6 - Adaptive Evolutionary System for Operating System Process Identification

6.1 Introduction 121  
6.2 Proposed Algorithm and Technology Used 123  
  6.2.1 Structure of Proposed Algorithm 124  
  6.2.2 Module 1: Generation of Detectors with the Help of GA 124  
6.3 Selection of Common Process’s Parameter 125  
  6.3.1 Range of Parameters 126  
  6.3.2 Structure of the Detectors 127  
6.4 Randomly Generated Detectors 128  
6.5 Generation of New Detectors with the Help of GA 129  
  6.5.1 Detector Generation Using One Point and Two Point Crossover 130  
  6.5.2 Detector Generation Using Uniform Crossover 135  
  6.5.3 Detector Generation Using Arithmetic Crossover and Heuristic Crossover 138  
6.6 Comparison of New Generated Detectors 143  
6.7 Experimental Results and Comparisons 143  
6.8 Identification of Non-Self Operating System Processes 144  
6.9 Summary 151
CHAPTER 7 - CONCLUSIONS AND SCOPE OF FUTURE WORK 153

APPENDIX – 1 ANALYSIS OF USER’S PROSPECTIVE ACTION 157
   A.1 INTRODUCTION 157
   A.2 POSSIBLE ACTIONS ON OS PROCESS 158
   A.3 END PROCESS IN WINDOWS OPERATING SYSTEM 159
   A.4 END A PROCESS IN UNIX OPERATING SYSTEM 162
   A.5 ACTIONS ON NON-SELF PROCESS OF OTHER OPERATING SYSTEMS 163
   A.6 SUMMARY 166

REFERENCES 167 -174