DANGER THEORY METAPHOR IN ARTIFICIAL IMMUNE SYSTEM FOR SYSTEM CALL DATA

ANJUM IQBAL

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

MAY 2006

ABSTRACT

Artificial Immune System (AIS) is a naive paradigm in biologically inspired computation; artificial neural networks (ANNs) and genetic algorithms (GAs) are among popular examples in this domain. The field of AIS research is vast and complex that demands immense multi-disciplinary efforts. As AIS is designed on the principles of natural Immune System (IS); so features of immune-inspired computational metaphors reflect features of the immunological theories/phenomena upon which these metaphors are based. In immunology, there are two distinct viewpoints about main goal of IS; "self-non-self" and "danger theory". Most of the existing AIS are based on classical self-non-self perspective. A recent recommendation has initiated some efforts exploring potentials of danger theory (DT) for AIS. A few existing DT based AIS metaphors are not sufficient to justify potentials of the vast field, so more explorations are needed. This study aims to contribute for the domain proposing a novel metaphor DASTON (DAnger Susceptible daTa codON). The effort completes four objectives; framework for abstracting immunology inspired computational metaphor, mechanism for DASTON abstraction, verifying existence of DASTON through benchmark data, and discovering novel biological property "bio fitness" for computational metaphors. Although, AIS is emerging as general paradigm for wide application area, computer security is its naturally analogous domain. So, exploitation of system call data, having enormous significance in computer security, is a good suggestion for this study. It concludes that; proposed framework is viable for abstracting immune-inspired metaphors, abstracted metaphor DASTON exists in system call data and fulfils proposed test criterion "bio-fitness" that proves its analogy to basis biological phenomena. The study also proposes a distinctive biological phenomenon "danger susceptibility" that might provide base for some useful immunological exploration. Hence, this thesis mainly contributes for DT based AIS with partial contributions for computer security, bio-inspired computation, and immunology.

ABSTRAK

Sistem Kebal Buatan (SKB) merupakan suatu paradigma yang agak naif dalam bidang perkomputeran berinspirasikan biologi; Rangkaian Neural Buatan (RNB) dan Algoritma Genetik (AG) adalah di antara contoh yang popular di dalam domain ini. Bidang SKB adalah sangat luas dan amat rumit, yang memerlukan suatu usaha yang tinggi di dalam pelbagai disiplin. SKB direkabentuk berasaskan kepada prinsip-prinsip tabii Sistem Kebal (SK); oleh yang demikian, ciri-ciri metafor pengkomputeran berinspirasikan konsep immunisasi menggarap ciri teori/fenomena imunilogikal ini yang menjadi asas kepada metafor ini. Dalam immunologi, terdapat dua pendapat yang jelas berkenaan matlamat SK ini iaitu *self-non-self* dan *Danger Theory (DT)*. Hampir kesemua penyelidikan SKB sedia ada menggunakan perspektif klasik iaitu *self-non-self*. Cadangan terkini telah mencetuskan beberapa usaha menjelajahi potensi DT di dalam SKB. Beberapa DT yang wujud berasaskan metafor SKB adalah tidak mencukupi untuk menjelaskan potensinya di dalam bidang yang luas. Oleh yang demmikian, penjelajahan lanjutan perlu dibuat. Kajian ini ialah bertujuan untuk menyumbang satu metafor yang baru iaitu DASTON (DAnger Susceptible daTa codON). Usaha ini menyumbang kepada penyelidikan SKB yang merangkumi empat objektif iaitu rangka kerja untuk melakukan pengabstrakan metafor pengkomputeran yang berinspirasikan immunologi, mekanisma umum terhadap pengabstrakan DASTON, menentusahkan kewujudan DASTON menerusi data perbandingan dan melakukan penemuan baru dalam bidang biologi iaitu *bio-fitness* untuk metafor perkomputeran. DASTON ini dijangka akan membuka satu lembaran baru dalam penyelidikan SKB. Walaupun SKB semakin berkembang sebagai paradigma umum untuk pelbagai aplikasi, bidang keselamatan komputer merupakan bidang yang lazimnya dikaitkan dengan domain SKB. Jesteru itu, penyelidikan ini telah mengekploitasikan data *system call* yang mempunyai impak yang sangat besar di dalam bidang keselamatan computer. Kajian ini merumuskan bahawa rangkakerja yang dicadangkan adalah baik dan praktikal, serta mampu melakukan pengabstrakan metafor pengkomputeran yang berinspirasikan immunologi, kewujudan pengabstrakan metafor DASTON di dalam data *system call*, dan memenuhi tahap kriteria cadangan *bio-fitness* iaitu dengan pembuktian kewajaran impaknya terhadap fenomena asas biologi. Kajian ini juga mencadangkan fenomena biologi yang khusus iaitu *danger susceptibility* yang mampu menyediakan asas yang berguna kepada penjelajahan imunologi lanjutan. Oleh yang demikian, sumbangan yang besar di dalam tesis ini adalah kepada *DT* berasaskan SKB, dengan sumbangan terhad terhadap bidang keselamatan komputer, pengkomputeran berinspirasikan biologi dan imunologi.

ABSTRAK

Sistem Kebal Buatan (SKB) merupakan suatu paradigma yang agak naif dalam bidang perkomputeran berinspirasikan biologi; Rangkaian Neural Buatan (RNB) dan Algoritma Genetik (AG) adalah di antara contoh yang popular di dalam domain ini. Bidang SKB adalah sangat luas dan amat rumit, yang memerlukan suatu usaha yang tinggi di dalam pelbagai disiplin. SKB direkabentuk berasaskan kepada prinsip-prinsip tabii Sistem Kebal (SK); oleh yang demikian, ciri-ciri metafor pengkomputeran berinspirasikan konsep immunisasi menggarap ciri teori/fenomena imunilogikal ini yang menjadi asas kepada metafor ini. Dalam immunologi, terdapat dua pendapat yang jelas berkenaan matlamat SK ini iaitu *self-non-self* dan *Danger Theory (DT)*. Hampir kesemua penyelidikan SKB sedia ada menggunakan perspektif klasik iaitu *self-non-self*. Cadangan terkini telah mencetuskan beberapa usaha menjelajahi potensi DT di dalam SKB. Beberapa DT yang wujud berasaskan metafor SKB adalah tidak mencukupi untuk menjelaskan potensinya di dalam bidang yang luas. Oleh yang demmikian, penjelajahan lanjutan perlu dibuat. Kajian ini ialah bertujuan untuk menyumbang satu metafor yang baru iaitu DASTON (DAnger Susceptible daTa codON). Usaha ini menyumbang kepada penyelidikan SKB yang merangkumi empat objektif iaitu rangka kerja untuk melakukan pengabstrakan metafor pengkomputeran yang berinspirasikan immunologi, mekanisma umum terhadap pengabstrakan DASTON, menentusahkan kewujudan DASTON menerusi data perbandingan dan melakukan penemuan baru dalam bidang biologi iaitu *bio-fitness* untuk metafor perkomputeran. DASTON ini dijangka akan membuka satu lembaran baru dalam penyelidikan SKB. Walaupun SKB semakin berkembang sebagai paradigma umum untuk pelbagai aplikasi, bidang keselamatan komputer merupakan bidang yang lazimnya dikaitkan dengan domain SKB. Jesteru itu, penyelidikan ini telah mengekploitasikan data *system call* yang mempunyai impak yang sangat besar di dalam bidang keselamatan computer. Kajian ini merumuskan bahawa rangkakerja yang dicadangkan adalah baik dan praktikal, serta mampu melakukan pengabstrakan metafor pengkomputeran yang berinspirasikan immunologi, kewujudan pengabstrakan metafor DASTON di dalam data *system call*, dan memenuhi tahap kriteria cadangan *bio-fitness* iaitu dengan pembuktian kewajaran impaknya terhadap fenomena asas biologi. Kajian ini juga mencadangkan fenomena biologi yang khusus iaitu *danger susceptibility* yang mampu menyediakan asas yang berguna kepada penjelajahan imunologi lanjutan. Oleh yang demikian, sumbangan yang besar di dalam tesis ini adalah kepada *DT* berasaskan SKB, dengan sumbangan terhad terhadap bidang keselamatan komputer, pengkomputeran berinspirasikan biologi dan imunologi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABRIVIATIONS

AIS	-	Artificial Immune System
Ab	-	Antibody
Ag	-	Antigen
APC	-	Antigen Presenting Cell
ANN	-	Artificial Neural Network
ARTIS	-	Artificial Immune System
CDIS	-	Computer Defense Immune System
CD	-	Compact Disk
CM	-	Computational Metaphor
CVIS	-	Computer Virus Immune System
DATAL	-	Data Allele
DASTAL	-	DASTON Associated Data Allele
DATON	-	Data Codon
DASTON	-	Danger Susceptible Data Codon
dsDNA	-	Double-Stranded DNA
DL	-	DASTON Associated Locus
*d*SOSDM	-	Dynamic Self Organizing Sparse Distributed Memories
CARDINAL	-	Cooperative Automated worm Response and Detection Immune Algorithm
DS	-	Danger Signal
DT	-	Danger Theory
ETDO	-	Evolutionary Time Dependent Optimization
GA	-	Genetic Algorithm
HIS	-	Human Immune System

HLA	-	Human Leukocyte Antigen
ICARIS	-	International Conference on Artificial Immune Systems
ID	-	Intrusion Detection
IDS	-	Intrusion Detection System
INS	-	Infectious Non Self
IS	-	Natural Immune System / Human Immune System
ISS	-	Information Security System
LISYS	-	Lightweight Intrusion Detection System
MHC	-	Major Histo-compatability Complex
MISA	-	Multi-objective Immune System Algorithm
PAMP	-	Pathogen Associated Molecular Patterns
PIC	-	Polymorphic Information Content
PICD	-	Polymorphic Information Content of DASTON
pH	-	Process Homeostasis
PH	-	Percent Hydrogen
PL	-	Polymorpic Locus
PRR	-	Pattern Recognition Receptor
SNP	-	Single Nucleotide Polymorphism
SNS	-	Self Non Self
(SAIS)	-	Simple Artificial Immune System
SOSDM	-	Self Organizing Sparse Distributed Memories
TDO	-	Time Dependent Optimization
TNF	-	Tumor Necrosis Factor
TSP	-	Traveling Salesman Problem
Th	-	Helper T-Cell
Tk	-	Killer T-Cell

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Natural systems are believed to be the best designed systems. The principles of natural systems are being followed in various fields of activity in effort to achieve the best possible results. The outcome depends upon the level of our understanding of the natural system and its proper application to a field. Applying the principles of natural systems is not a naive approach. The natural systems have been source of inspiration since ancient times in different fields including, engineering, economics, sociology, education, defense, and many more. Recently the trend of following natural systems, especially biological systems, has increased. It may be due to increased understanding of highly sophisticated biological systems. The computational and biological sciences are delivering benefits to each other (see Figure 1.1); principles of biological systems help in abstracting novel computational mechanisms, and modern computational powers help in better and quick understanding of biological processes. The two folds applications of biology and computation has wired these fields into strong link. The link that will grow complex but more useful as the research will progress. This link will involve the contributions from many disciplines; computer science, mathematics, physics, engineering, biology, bioinformatics, and many others. The field of computation has strong history of proven successes from biological inspirations. The artificial neural networks, genetic algorithms, evolutionary programming, and recently introduced artificial immune system must be quoted as examples.

1.2 Artificial Immune System Overview

Artificial Immune System (AIS) is relatively naïve paradigm in computational field (Forrest and Perelson, 1992). The AIS is a computational system designed on the principles of natural immune system (IS) (Somayaji *et al*., 1998). The immune system performs the duty of protecting humane body from harmful elements and events. The story of AIS research starts from wet immunology research labs where immunologists perform experiments in-vitro (in test tubes) and in-vivo (in

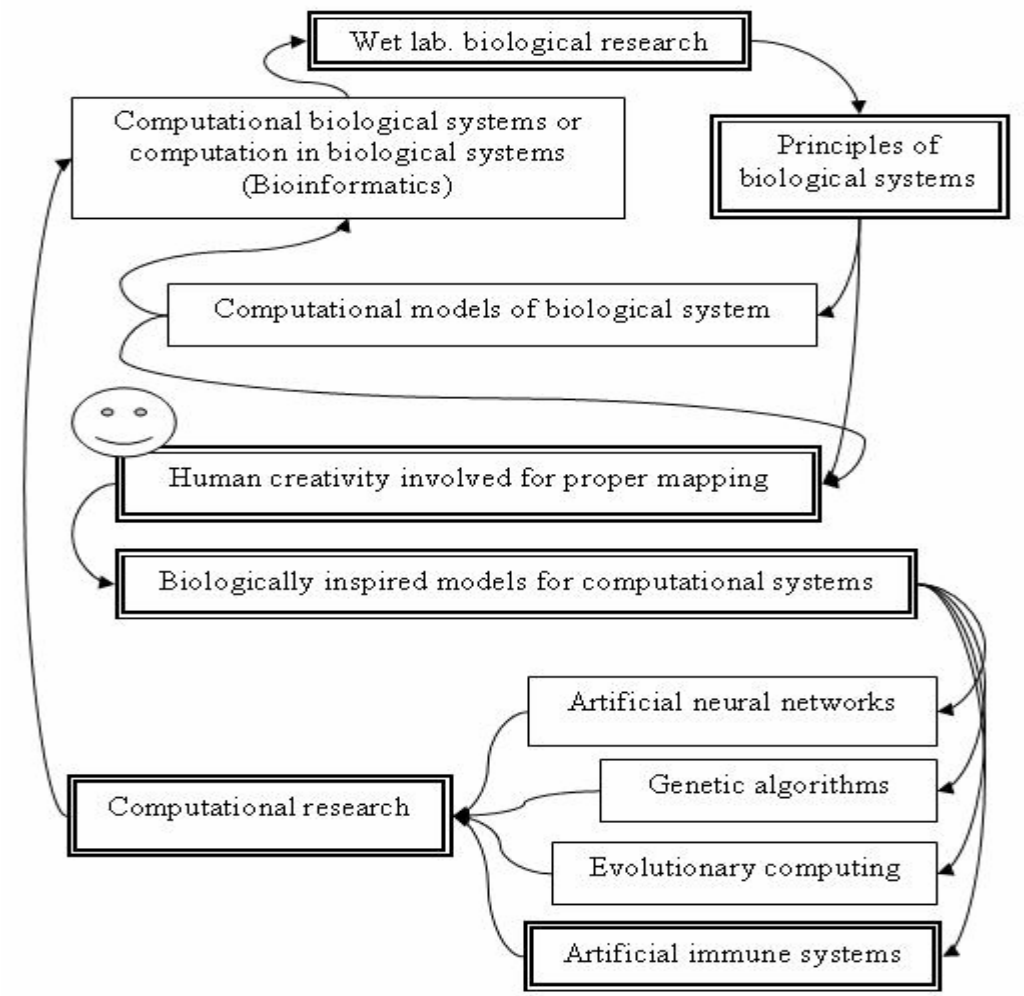

Figure 1.1: Research process for biological inspired computation

test organisms). They reveal the principles of immune system. The computational researchers can utilize these principles in two ways; computational models can be designed to mimic the immunological processes for in-silico (in computers) immunology research also called immuno-informatics, and novel metaphors can be abstracted and mapped to computational systems called artificial immune systems, see Figures 1.1 and 1.2.

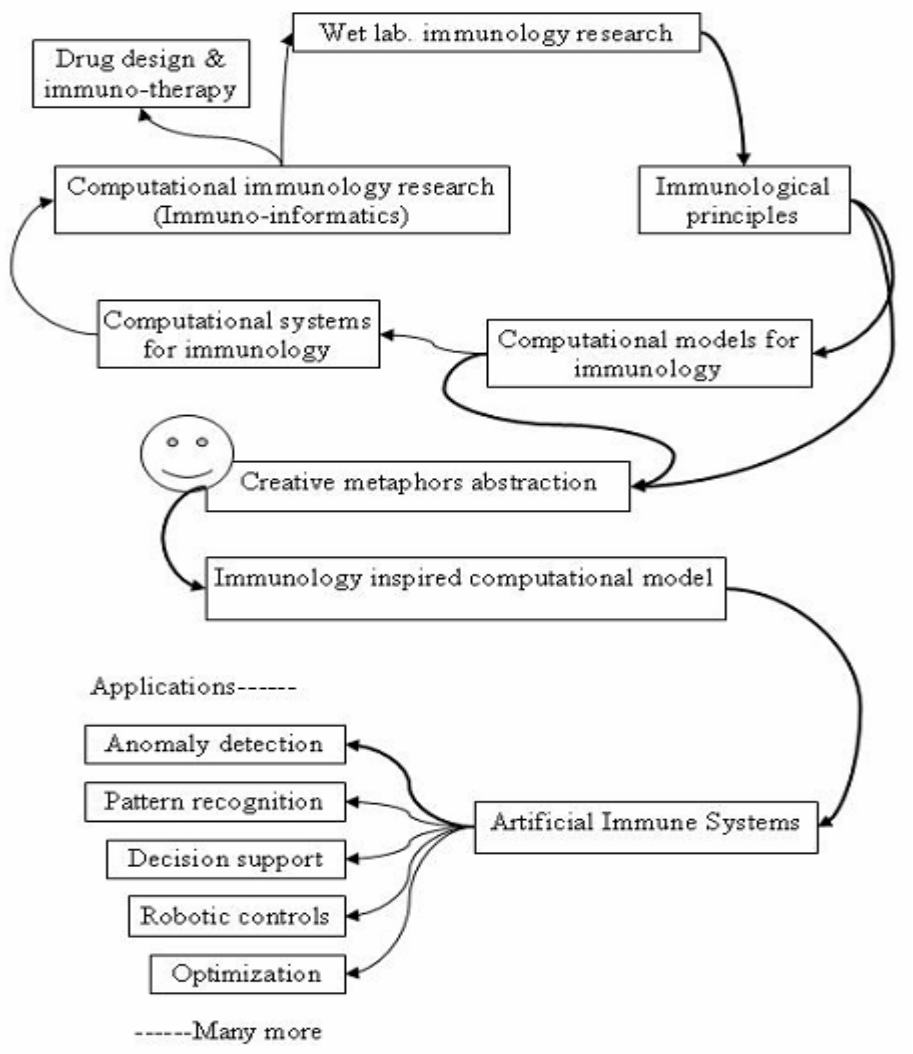

Figure 1.2: Research process for immune inspired computation

1.3 Distinct Approaches in Artificial Immune System Research

As described earlier Artificial Immune System (AIS) is a computational system designed on the principles of natural immune system (IS). In immunology, there are two distinct viewpoints about the main goal of immune system; the classical *self-non-self viewpoint* states that immune system discriminates between self (human body cells and molecules) and non-self (other invading cells and molecules), and the *danger theory viewpoint* describes that the immune system looks for dangerous elements and events whether self or non-self (Matzinger, 2002), see Figure 1.3.

The two viewpoints, though controversial among immunologists, are providing guidelines for designing better artificial immune systems (Aickelin and Cayzer, 2002). The most of the existing AIS research is based on self-non-self viewpoint (Forrest *et al.,* 1994, 1996). There are only a few preliminary efforts (see next section 1.4) witnessing potentials of Danger Theory for AIS research. The focus

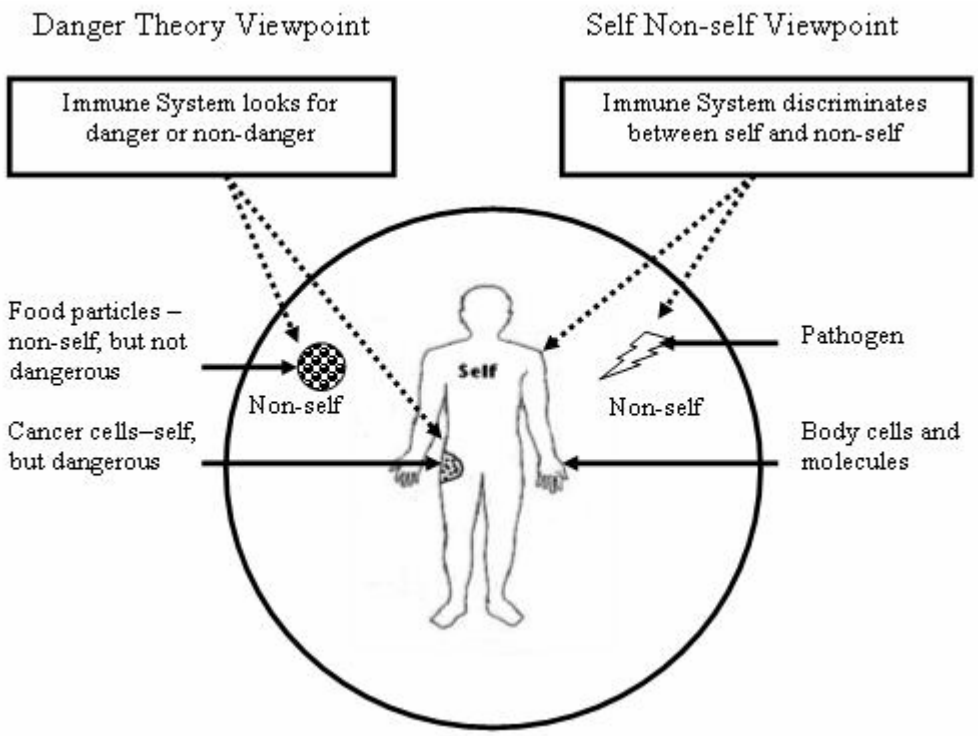

Figure 1.3: Two viewpoints about the main goal of immune system

of the study, described in this thesis, is to further elaborate the potentials of danger theory for artificial immune systems.

1.4 Need for Danger Theory based AIS Metaphors

The recommendation of Aickelin and Cayzer (2002) has motivated some AIS practitioners to explore the potentials of danger theory (Matzinger, 1998, 2001a, 2001b, 2002). For being novel and emotive idea we can see only a few efforts till recently. The pioneering danger theory (DT) based AIS research is more focusing on the philosophical foundation of the idea, so to establish tangible base for future applied research. The existing DT based metaphors are not enough, in terms of quantity and maturity, to justify its potentials for AIS. This section is to perceive the latest status of DT based AIS research which persuades the need for concrete metaphors in this domain (please refer section 3.5 chapter 3 for some details and respective literature for further details).

Aickelin and Cayzer (2002) initiated the idea of exploiting DT for AIS. The primary focus of the idea is about creating a next generation IDS (intrusion detection system). They have described the issues pertaining to self-non-self with an example of "negative selection" and respective DT based proposal to establish base for their idea. The subsequent efforts (Aickelin *et al*., 2003, 2004) also meant to emphasize the use of DT approach for AIS. These are good preliminary concepts that tell how DT inspiration can be employed to develop metaphors for AIS.

Hart and Ross (2003) received motivation for DT to improve their original SOSDM (Self Organizing Sparse Distributed Memories) algorithm (Hart and Ross, 2002). The improved algorithm, *d*SOSDM (dynamic SOSDM), was more able to deal with dynamically changing environments (Hart and Ross, 2003). They used the idea of contentment of antibodies in a dangerous environment. Secker *et al*. (2003) presented a concept to explore the relevance of DT to the application domain of web mining; the idea was originally initiated in (Aickelin and Cayzer, 2002). The authors

(Secker *et al*., 2003) argue that DT suggests context dependant response to invading pathogens, which could be utilized as metaphor for applications in web mining.

The goal of (Sarafijanovic and Boudec, 2004) is to build an AIS that, like its natural counterpart, automatically learns and detects new misbehavior in ad-hoc networks. In this effort Danger Signal (DS) model has been applied to protect "dynamic self", the self that is dynamically determined through the interaction of nodes and feedback in form of losses. Greensmith *et al*. (2005) have used the functionality of Dendritic cells as a metaphor to derive an algorithm. These cells are antigen presenting cells (APC) that play central roll in receiving and transmitting danger-signals. The preliminary results of the algorithm on breast cancer data show hopeful classification of the data. The similar idea of modeling an APC was initiated in (Iqbal and Maarof, 2004).

In the study of (Kim *et al*., 2005) numerous mechanisms inspired from the differentiation states of T-cells have been adopted to propose AIS model CARDINAL (Cooperative Automated worm Response and Detection ImmuNe ALgorithm). The role of T-cells is to confirm and assess anomalous situations and then either respond to or tolerate the source of the effect. Bentley *et al*. (2005) introduce "tissue-paradigm" as an interface between problem domain and AIS. They propose that tissue designed for artificial immune algorithms should comprise a series of linked cells, each cell "grown" in response to specific data, in a data stream being input to AIS. This metaphor is inspired from danger model in such that danger is presented to the immune system through tissue damage.

All of the existing DT based AIS metaphors described in above paragraphs are at their preliminary stages. These show that danger theory perspective of immune system can be exploited to derive variety of metaphors for AIS. The existing metaphors observe only a few of the DT mechanisms; also these metaphors are not mature enough to fully justify the potential of the idea. Therefore, numerous metaphors covering various aspects of the idea are required for its support. Then we might be able to strongly justify the potentials of DT for AIS.

1.5 Research Goal and Objectives

This study aims to explore the potentials of Danger Theory for Artificial Immune Systems proposing a novel immunology inspired computational metaphor called DASTON (DAnger Susceptible daTa codON) based on proposed biological phenomenon “danger susceptibility”. The following objectives have been completed in the study;

- Framework for abstracting immunology inspired computational metaphor
- Abstraction of novel danger theory inspired computational metaphor
- Identification of the metaphor in system call data
- Exploration of novel biological property of the computational metaphor

The artificial immune system is naive, multidisciplinary and relatively less explored field. It demands a carefully designed study for significant contribution. The four objectives are pilled up to contribute for the main goal of this study.

The first objective - framework for abstracting immunology inspired computational metaphor - is to sketch a framework that serves as a guide map for abstracting immunology based computational metaphor. This framework is important to have structured approach in abstracting metaphor. This objective provides base for the subsequent objectives, which verify the worth of the framework.

The second objective – abstraction of novel danger theory inspired computational metaphor - The success of this objective is hidden in appropriate mapping of immunological/biological concepts to computational field. Supported by established biological theories; danger theory, infectious disease susceptibility, and host pathogen interaction, a new phenomenon “danger susceptibility” has been proposed. The proposed metaphor DASTON is a product of suitable mapping of “danger susceptibility” to computational mechanism. The following objectives confirm existence of DASTON in computational data and strength of the mapping.

The third objective - identification of novel computational metaphor - is to propose a mechanism for identifying DASTONs in a particular application area. This study opt intrusion detection as a case study. The data set used is system calls bench mark data. The existence of DASTONs in system call data validates the metaphor and the respective identification mechanism.

The fourth objective – exploration of biological property of the computational metaphor - is to prove that the computational metaphor DASTON holds good analogy with its biological counter parts. It has been proven that the DASTON (though computational metaphor) holds biological property. We define the term "bio-fitness" for DASTON reflecting proper mapping in two distinct fields.

1.6 Research Motivation

The basic motivation for studying immune system was received from the book titled "The Miracle of The Immune System" (Yahya, 2001). The attractive description of human immune system in that book enhanced my thirst for studying immune system and mapping its principles to computational systems. That was inspiring start of this research for artificial immune systems. The other motivational factors for this research are described in following paragraphs.

Artificial immune system in infancy **-** The field of artificial immune system is currently in its infancy and requires enormous efforts to build strong general skeleton. Most of the existing AIS models are meant mainly for computer security applications (Dasgupta, 1999; Hofmeyr, 1999; Kim and Bentley, 1999; Lei and Hirsbrunner, 2002; Paula *et al.,* 2002; Skormin *et al.,* 2001; Williams *et al*., 2001). This is because computer security is the most natural domain to begin applying immune system mechanisms. In computer security, the analogy between protecting the body and protecting a normally operating computer is evident (Hofmeyr, 2000). This research might be a good exercise abstracting and exploring a novel AIS metaphor with reference to computer security.

The novel viewpoint about immune system - Existing AIS research is mainly focusing the classical self-non-self viewpoint, which is more popular among immunologists. Aickelin and Cayser (2002) urge that novel danger theory viewpoint should be explored. Currently, only a few research efforts (see section 1.4) have been initiated in this domain, which offer enough room for significant contributions.

An email from AIS guru - Following is the inspiring email reply from Aickelin (2002), the pioneer of the idea that danger theory could deliver useful metaphors for AIS:

Tue, 29 Jul 2003
Hello,
As the danger theory (DT) is new and still vague, I have yet to see any mathematical models.
Good general references are the 1994 paper by Matzinger and her latest papers (since 2000). There are a number of the newer ones, all quite similar. Also keep your eyes open for latest papers in this year ICARIS 2003; there will be a few on the DT. (I have attached my latest work).
Your work sounds interesting, please keep me informed.
Best, Uwe Aickelin.

Support of ARTIST and ICARIS – The ARTIST is an academic network of AIS researchers and ICARIS is the International Conference on Artificial Immune Systems, which is the only worldly renowned platform dedicated for quality AIS research. The first ICARIS was held in September 2002. This study received bursary awards from ARTIST to attend ICARIS-2003 and to present research papers in ICARIS-2004 and 2005. To encourage AIS research in Malaysia, the ARTIST partly sponsored the International Symposium on Bio-Inspired Computation (BIC'05) (website - http//bic05.fsksm.utm.my)

Complexity, difficulty, and significance - the immune system (IS) is a complex biological system. The mapping of IS mechanisms to computational systems demands multidisciplinary knowledge that increases the level of difficulty. The significance of AIS research is that, it is steadily growing as core knowledge in

artificial intelligence with wide application area. It is the time to be in pace with AIS research for learning fundamentals and presenting novel contributions.

Marriage of immunology and computational science - both biology and computation are entirely distinct sciences, but their marriage delivers promising benefits to both. The use of computational power and techniques in immunology gives rise to immuno-informatics or *insilico* immunology, while better understanding of immune system exposes novel AIS metaphors. AIS practitioner may serve as a bridge between immunologists and computational scientists to cope the problem of mutual understanding (Kim, 2002).

1.7 Research Contributions

This research mainly aims to reveal the potential of danger theory for artificial immune system research. The four research objectives (stated in section 1.5) have been completed with distinct contributions, briefly described in following paragraphs.

Framework to abstract immune inspired metaphor – the framework provides guidelines for abstracting immune inspired computational metaphor. This contribution builds a base for subsequent contributions; conversely, the following contributions verify the significance of the framework.

Novel computational metaphor – this contribution is based on the knowledge obtained from the first contribution, and deep literature reviews in biology, immunology, genetics, intrusion detection, system calls analysis, and other related fields. It is the most critical part of the study. The effort proposes a computational metaphor called DASTON (DAnger Susceptible daTa codON) based on proposed idea of "danger susceptibility". The DASTON has strong analogies with biological counterparts.

Mechanism to identify DASTON – As the concept of DASTON is novel and relatively complex, therefore the mechanism of identifying DASTON requires an application field strongly analogous to the biological counterparts. This research applies the concept to system calls bench mark data (http://www.cs.unm.edu/). The system calls data has significance in intrusion detection (computer security) applications. The effort successfully shows the presence of DASTONs in system calls data by processing normal and intrusion trace system call sequences.

Biological property of computational metaphor (bio-fitness) - the basis of this research is a controversial immunological theory, danger theory. This research does not advocate the immunological theories but tries to get benefits of that proving the strength of DASTON. Interestingly, the computational metaphor DASTON bears the biological property of polymorphism. This property also proves that how close is the computational metaphor to its biological counterparts. It also suggests a novel criterion "bio-fitness" for evaluating a biologically inspired computational metaphor.

1.8 Thesis Organization

The thesis has been organized to elaborate the major aspects addressed in this complex multidisciplinary study. Following paragraphs give a brief overview of the thesis.

Chapter 2 gives an overview of natural immune system and distinct viewpoints about its main goal, that is, "self-no-self" and "danger theory". This is to cover essential topics in immunology related to artificial immune system (AIS) study presented in this thesis.

Chapter 3 provides an overview of the AIS and review of the related literature. It describes how AIS researchers are motivated for DT metaphors exploration. This chapter also presents the existing danger theory based AIS metaphors. These preliminary metaphors are a few in numbers, demanding more to justify potentials of DT for AIS.

Chapter 4 gives the general description of method used to achieve objectives of this study. It elaborates the framework for abstracting immunology inspired computational metaphor. This framework provides the basic guidelines for the process of metaphor abstraction.

Chapter 5 portrays the process of abstracting the novel computational metaphor DASTON. The biological phenomena; danger theory, infectious disease susceptibility, and host-pathogen interaction have been described to propose a new concept of "danger susceptibility" as a base for DASTON abstraction.

Chapter 6 describes the method to identify DASTONs in system calls bench mark data. It also demonstrates experimental results proving presence of DASTONs in the said data.

Chapter 7 explores the biological property (polymorphism) and proposes a novel test criterion (bio-fitness) of computational metaphor DASTON. It presents the experimental results witnessing that a computational metaphor holds biological property, which is an interesting exploration of this research.

The thesis concludes in chapter 8, expressing; the point of view established by this study about AIS research, novel contributions of the thesis, and future directions for the related research.

1.9 Summary

This chapter gives the overview of the study briefly describing artificial immune system (AIS), the distinct approaches (self-non-self and danger theory) for AIS research, need for danger theory based AIS metaphors, research goal and objectives, research motivation, research contributions, and organization of the whole thesis. This study hopes to motivate researchers for multidisciplinary AIS research.

BIBLIOGRAPHY

Adarichev, V. A., Bárdos, T., Christodoulou, S., Phillips, M. T., Mikecz, K., and Glant, T. T. (2002). Major Histocompatibility Complex Controls Susceptibility and Dominant Inheritance, but Not the Severity of the Disease in Mouse Models of Rheumatoid Arthritis. *Immunogenetics.* 54:184–192.

Adrian, V. S. H. (1999). Genetics and Genomics of Infectious Disease Susceptibility. *British Medical Bulletin.* 55(2): 401-413.

Aickelin, U., Greensmith, J., Twycross, J. (2004). Immune System Approaches to Intrusion Detection - A Review. *Proceedings of the 3rd International Conference on Artificial Immune Systems (ICARIS, 2003)*

Aickelin, U., Bentley, P., Cayser, S., Kim, J., and Mc Leod, J. (2003). Danger Theory: The Link between AIS and IDS. *Proceedings of the 2nd International Conference on Artificial Immune Systems (ICARIS, 2003).* September 1-3. Edinburgh, UK.

Aickelin, U., and Cayzer, S. (2002). The Danger Theory and Its Application to Artificial Immune Systems. *Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS, 2002).* September 9-11, Canterbury, UK. Tomorrow

Almgren, M., and Lindqvist, U. (2001). Application-Integrated Data Collection for Security Monitoring. In: Lee, W., M´e, L., and Wespi, A. eds. *RAID 2001, LNCS 2212, Springer-Verlag*. Berlin Heidelberg. 22-36.

Anchor, K. P., Williams, P. D., Gunsch, G. H., and Lamont, G. B. (2002). The computer defense immune system: current and future research in intrusion detection. Proceedings of the Congress on Evolutionary Computation (CEC '02). May 12-17. Honolulu, HI. 2: 1027 –1032.

Antoniol, G., Fiutem, R., and Cristoforetti, L. (1998). Using Metrics To Identify Design Patterns In Object-Oriented Software. *Proceedings of Fifth International Software Metrics Symposium.* November 20-21, 1998, Bethesda, Maryland: IEEE, 23 – 34.

Arakawa, T., Carninci, P., and Kawai, J. (2003). Identification of Putative Noncoding RNAs Among the RIKEN Mouse Full-Length cDNA Collection. *Genome Research*. 13:1301–1306.

Arup, K. C., Michael, L. D., and Andrey, S. S. (2003). In-silico Models for Cellular and Molecular Immunology: Successes, Promises and Challenges. *Nature Immunology*. 4: 933-936.

Arup, K. C. (2002). Lighting up TCR Takes Advantage of Serial Trigring. *Nature Immunology*. 3: 895-896.

Asaka, M., Onabora, T., Inoue, T., and Goto, S. (2002). Remote Attack Detection Method in IDA: MLSI-Based Intrusion Detection using Discriminant Analysis. *Proceedings of the IEEE International Symposium on Applications and Internet (SAINT2002).* Jan.28-Feb.1. Nara, Japan.

Asaka, M., Onabora, T., Inoue, T., Okazawa, S., and Goto, S. (2001). A New Intrusion Detection Method Based on Discriminant Analysis. *IEICE Transactions on Information and Systems.* E84-D(5): 570-577.

Asaka, M., Taguchi, A., Goto, S. (1999). The Implementation of IDA: An Intrusion Detection Agent System. *Proceedings of the 11th FIRST Conference 1999.* Brisbane, Australia.

Asaka, M., Okazawa, S., Taguchi, A., Goto, S. (1999). A Method of Tracing Intruders by Use of Mobile Agent. *Proceedings of the 9th Annual Internetworking Conference (INET`99).* San Jose, California.

Athanasiades, N., Abler, R., Levine, J., Owen, H., and Riley, G. (2003). Intrusion Detection Testing and Benchmarking Methodologies. *Proceedings of the First IEEE International Information Assurance Workshop (IWIA'03).* March 24-24. Darmstadt, Germany.

Aversano, L., Canfora, G., De Lucia, A., and Stefanucci, S. (2002). Evolving Ispell: A Case Study of Program Understanding for Reuse. *Proceedings of 10th International Workshop on Program Comprehension.* June 26-29. La Sorbonne, Paris, France: 197- 206.

Baas, A., Gao, X., Chelvanayagam, G. (1999). Peptide Binding Motifs and Specificities for HLA-DQ Molecules. *Immunogenetics.* 50: 8–15

Bace, R., and Mell, P. (2001). Intrusion Detection Systems. Special Publication 800-31. National Institute of Standards and Technology (NIST).

Baggish, J., and MacNeill, S. (1994). How Your Immune System Works. Emeryville, CA : Ziff-Davis Press, 1994

Balthrop, J., Esponda, F., Forrest S., and Glickman, M. (2002). Coverage and Generalization in an Artificial Immune System. *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 2002).* July 9-13. New York: 3-10.

Balthrop, J., Forrest, S., Glickman, M. (2002). Revisiting LISYS: Parameters and Normal Behavior. *Proceedings of the 2002 Congress on Evolutionary Computation.* May 12-17. Honolulu, Hawaii.

Banchereau, J., and Steinman, R. M. (1998). Dendritic Cells and the Control of Immunity. *Nature*. 392: 245-252.

Barry, P. J. (2002). Intrusion Detection – Evolution beyond Anomalous Behavior and Pattern Matching. *Security Essentials*. Version 1.4.

Basu, S. Binder, R. J., Suto, R., Anderson, K. M., and Srivastava, P. K. (2000). Necrotic but not Apoptotic Cell Death Releases Heat Shock Proteins, Which Delivers a Partial Maturation Signal to Dendritic Cells and Activate the NF-kB Pathway. *International Immunology*. 12(11):1539-1546.

Basu, C., Hirsh, H., and Cohen, W. W. (1998). Recommendation as Classification: Using Social and Content-Based Information in Recommendation. Proceedings of the Fifteenth National Conference on Artificial Intelligence and Tenth Innovative Applications of Artificial Intelligence Conference (AAAI 98). July 26-30. Madison, Wisconsin, USA. 714-720.

Beauchemin, C. (2002). Modelling the Immune System. *Technical Report.* Department of Physics, University of Alberta.

Begnum, K., and Burgess, M. (2003). A Scaled, Immunological Approach to Anomaly Countermeasures (Combining Ph with Cfengine). *Integrated Network Management*. 2003: 31–42

Bentley, P. J., Greensmith, J., and Ujjin, S. (2005). Two Ways to Grow Tissue for Artificial Immune Systems. *Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS-2005),* (In Print).

Bernaschi, M., Gabrielli, E., and Mancini, L. V. (2000). Linux Kernel Enhancements for Immediate Intrusion Detection.

Bernaschi, M., and Castiglione, F. (2001). Design and implementation of an immune system simulator. *Computers in Biology and Medecine.* 31(5): 303-331.

Blackwell, J. (2002), Genetics and Genomics in Infectious Disease, *CIMR Research Report*. Last accessed on 06-04-04. URL:http://www.cimr.cam.ac.uk/resreports/report2002/pdf/blackwell_low.pdf

Bleek, G. M. V., and Nathenson, S. G. (1991). The Structure of the Antigen-Binding Groove of Major Histocompatibility Complex Class I Molecules Determines Specific Selection of Self-Peptides. *Immunology*. 88:11032-11036.

Borghans, J. A. M., Beltman, J. B., and De Boer, R. J. (2004). MHC Polymorphism under Host-Pathogen Coevolution. *Immunogenetics*. 55:732–739.

Boudec, J., and Sarafijanovic, S. (2003). An artificial immune system approach to misbehavior detection in mobile ad-hoc networks. *Technical Report IC/2003/59*. Ecole Polytechnique Federale de Lausanne, 2003.

Branden, C., and Tooze, J. (1991). *Introduction to Protein Structure*. Garland Publishing Inc., New York and London.

Brian, D. B., and David, L. (2002). Dangerous Liaisons: The Role of "Danger" Signals in the Immune Response to Gene Therapy. *Blood.* 100(4): 1133-1139.

Burgess, M. (1998). Computer immunology. In Proc. of the Systems Administration Conference (LISA-98), pages 283–297, 1998.

Burnet, F. M. (1960). Immunological Recognition of Self. *Nobel Lecture*. December 12, 1960.

Byrne, E. J., and Gustafson, D. A. (1992). A Software Re-Engineering Process Model. *Proceedings of Sixteenth Annual International Computer Software and Applications Conference, Compsac '92.* September 22-25. Chicago, USA: IEEE, 25 – 30.

Byrne, E. J. (1992). A Conceptual Foundation for Software Re-Engineering. *Proceedings of Conference on Software Maintenance.* November 9-12. Orlando: IEEE, 226 – 235.

Can, K., Vera, V. N., Rob, J. D. B., and Paulien, H. (2003). Bioinformatic analysis of functional differences between the immuno-proteasome and the constitutive proteasome. *Immunogenetics*. 55: 437–449.

Cano, P., and Fan, B. (2001). A geometric and algebraic view of MHC-peptide complexes and their binding properties. *BMC Structural Biology.* 1(2).

Carlos, A., Coello, C., and Cortés, N. C. (2002). Solving Multiobjective Optimization Problems using an Artificial Immune System, *Technical Report EVOCINV-05-2002.* Evolutionary Computation Group at CINVESTAV, Sección de Computación, Departamento de Ingeniería Eléctrica, CINVESTAV-IPN, México.

Carvalho, D. R., and Freitas, A. A. (2001). An Immunological Algorithm for Discovering Small-Disjunct Rules in Data Mining. *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO-2001).* July 7-11, San Francisco, California.

Carver, C. A., Hill, J. M. D., and Pooch, U. W. (2001). Limiting Uncertainty in Intrusion Response. *Proceedings of the 2nd IEEE Systems, Man and Cybernetics Workshop on Information Assurance and Security.* June 5-6. West Point, NY.

Casadevall, A., and Pirofski, L. A. (2004). The Weapon Potential of a Microbe. *TRENDS in Microbiology*. 12(6): 259-263.

Casadevall, A., and Pirofski, L. A. (2004). New Concepts in Antibody-Mediated Immunity. *Infection and Immunity*. 72(11):6191–6196.

Casadevall, A., and Pirofski, L. A. (2003). Anti-Virulence' Genes – Further Muddling The Lexicon? *TRENDS in Microbiology*. 11(9): 413-414.

Casadevall, A., and Pirofski, L. A. (2001). Host-Pathogen Interactions: The Attributes of Virulence. *The Journal of Infectious Diseases*.184:337–44.

Casanova, J. L. (2001). Mendelian Susceptibility to Mycobacterial Infection in Man. *Swiss Med Weekly*. 131: 445–454.

Casadevall, A., and Pirofski, L. A. (2000). Host-Pathogen Interactions: Basic Concepts of Microbial Commensalism, Colonization *Infection and Disease*. 68(12): 6511–6518.

Casadevall, A., and Pirofski, L. A. (1999). Host-Pathogen Interactions: Redefining the Basic Concepts of Virulence and Pathogenicity. *Infection and Immunity*. 67(8): 3703–3713.

Christensen, D. (1999). Beyond Virtual Vaccinations. *Science News*. 156(5): 76.

Chun, J. S., Jung, H. K., and Hahn, H. Y. (1998). A Study on Comparison of Optimization Performances between Immune Algorithm and other Heuristic Algorithms. *IEEE Transanctions on Magnetics*. 34(5): 2972-2975.

Cochran, J. R., Cameron, T. O., and Stern, L. J. (2000). The Relationship of MHC-Peptide Binding and T Cell Activation Probed UsingChemically Defined MHC Class II Oligomers. *Immunity*. 12: 241–250.

Clancy, J. (1998). Basic Concepts In Immunology : A Student's Survival Guide. New York : McGraw-Hill, 1998

Cohn, M. (2005). A biological context for the Self-Nonself discrimination and the regulation of effector class by the immune system. *Immunol Research*. 31(2):133-50

Cohen, W. W. (1996). Learning Trees and Rules with Set Valued Features. *Proceedings of the Thirteenth National Conference on Artificial Intelligence (AAAI-96).* August 4 – 8. Portland, Oregon.

Cohen, W. W., and Kudenko, D. (1997).Transferring and Retraining Learned Information Filters. Proceedings of the Fourteenth National Conference on Artificial Intelligence and Ninth Innovative Applications of Artificial Intelligence Conference (AAAI 97). July 27-31. Providence, Rhode Island.

Cohen, W. W., Singer, Y. (1999). A Simple, Fast, and Effective Rule Learner. Proceedings of the Sixteenth National Conference on Artificial Intelligence (AAAI99). July 18-22. Orlando, Florida, USA.335-342.

Coussens, P. M., Tooker, B., Nobis, W., and Coussens, M. J. (2001). Genetics and Genomics of Susceptibility to Mycobacterial Infections in Cattle. On-line publication on the 2001 IAAFSC web site. Sited on 17-10-2004. URL:http://www.fass.org/fass01/pdfs/Coussens.pdf

Dasgupta, D. (2004). Immuno-Inspired Autonomic System for Cyber Defense. Computer Science Technical Report. 2004.

Dasgupta, D., Cao, Y., and Yang, C. (1999). An Immunogenetic Approach to Spectra Recognition. *Proceedings of the International Conference Genetic and Evolutionary Computation (GECCO).* July 13-17. Orlando: 149-155.

Dasgupta, D. (1999). Immunity-Based Intrusion Detection Systems: A General Framework. *Proceedings of 22nd National Information Systems Security Conference (NISSC).* October 18-21. Arlington, Virginia.

Dasgupta, D. (1997). Artificial Neural Networks and Artificial Immune Systems: Similarities and Differences. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics.* October 12-15. Orlando.

Dasgupta, D. (1999). Immunity-Based Intrusion Detection Systems: A General Framework. *Proceedings of 22nd National Information Systems Security Conference (NISSC)*. October 18-21. Arlington, Virginia.

Dasgupta, D (1999). Information Processing Mechanisms of the Immune System. In: Corne, D., Dorigo, M., Glover, F. Ed. *New Ideas in Optimization.* McGraw-Hill.1999.

Dasgupta, D. (1998). An Artificial Immune System as a Multi-Agent Decision Support System. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC).* San Diego. October 11-14, pp. 3816-3820, 1998

Dasgupta, D. (1996). Using Immunological Principles in Anomaly Detection. *Proceeding of the Artificial Neural Networks in Engineering (ANNIE'96).* 443-448. 1996

Dasgupta, D., and Forrest, S. (1996). Novelty Detection in Time Series Data Using Ideas from Immunology. *Proceedings of the 5th International Conference on Intelligent Systems*, Reno, June, 1996 http://www.msci.memphis.edu:80/~dasgupta/*publications*.html

Dausset, J. (1980). The Major Histocompatibility Complex In Man -- Past, Present, and Future Concepts. Nobel Lecture. University of Paris VII. 8 December, 1980

David, J. G. (2004). Immunomics: principles and practice. *IRTL Reviews*. 2: 1-6.

Davies, H. (1997). Introductory Immunobiology. London : Chapman & Hall, 1997

Davies, M. N., Sansom, C. E., Beazley, C., and David S Moss, D. S. (2003). A Novel Predictive Technique for the MHC Class II Peptide–Binding Interaction. Molecular Medicine. 9 (9-12): 220-225.

De Alboran, I. M., Baena, E., and Martinez-A, C. (2004). C-Myc-Deficient B-Lymphocytes are Resistant To Spontaneous and Induced Cell Death. *Cell Death and Differentiation*.11: 61–68.

De Boer, R. J., Borghans, J. A. M., Boven, M. V., Kesmir, C., and sing, F. J. (2004). Heterozygote Advantage Fails To Explain The High Degreeof Polymorphism Of The MHC. *Immunogenetics.* 55:725–731.

De Castro, L. N., Von Zuben, F. J. (1999). Artificial Immune Systems: A Survey of Applications. *Technical Report Part-1, TR – DCA 01/9.* State University of Campinas, SP, Brazil.

De Castro, L. N., Von Zuben, F. J. (2000a). Artificial Immune Systems: A Survey of Applications. *Technical Report Part-2, DCA–RT 02/00.* State University of Campinas. SP, Brazil.

De Castro, L. N., Von Zuben, F. J. (2000b). Leandro Nunes de Castro and Fernando J. Von Zuben. The clonal selection al-gorithm with engineering applications. *In Workshop Proceedings of GECCO'00*, Workshop on Artificial Immune Systems and their Applications. 36–37, Las Vegas, USA, July 2000.

De Castro, L. N., Von Zuben, F. J. (2001). aiNet: An Artificial Immune Network for Data Analysis", (full version, pre-print), Book Chapter in *Data Mining: A Heuristic Approach*, H. A. Abbass, R. A. Sarker, and C. S. Newton (eds.), Idea Group Publishing, USA, Chapter XII, pp. 231-259.

De Castro, L. N., and Timmis, J. I. (2002). Artificial Immune Systems: A Novel Paradigm to Pattern Recognition. In: Alonso, L., Corchado, J., and Fyfe, C. ed. *Artificial Neural Networks in Pattern Recognition*. University of Paisley. 67-84.

Debaud, J. M., and Rugaber, S. (1995). A Software Re-Engineering Method Using Domain Models. *Proceedings of International Conference on Software Maintenance.* October 17-20. Opio (Nice), France: IEEE, 204 – 213.

Decker, E. H. (2004). Self-Organizing Systems: A Tutorial in Complexity.

Delanoue, R., Legent, K., Godefroy, N., Flagiello, D., Dutriaux, A., Vaudin, P., Becker, J. L., and Silber, J. (2004). The Drosophila Wing Differentiation Factor Vestigial–Scalloped Is Required for Cell Proliferation and Cell Survival at the Dorso-Ventral Boundary of the Wing Imaginal Disc. *Cell Death and Differentiation*. 11: 110–122.

Denny, P., Hopes, E., Gingles, N., Broman, K. W., Mc Pheat, W., Morten, J., Alexander, J., Andrew, P. W., and Brown, S. D. M. (2003). A major Locus conferring Susceptibility to Infection by Streptococcus Pneumoniae in Mice. *Mammalian Genome, Springer.* 14: 448–453.

D'haeseleer, P. (1997). A Distributed Approach to Anomaly Detection. *ACM Transactions on Information System Security*, 1997
URL: http://www.cs.unm.edu/~patrik/

Dönnes, P., and Elofsson, A. (2002). Prediction of MHC Class I Binding Peptides, Using SVMHC. *BMC Bioinformatics.* 3(25).

Dziembowska, M., Fondaneche, M. C., Vedrenne, J., Barbieri, G., Wiszniewski, W., Picard, C., Cant, A. J., Steimle, V., Charron, D., Alca-Loridan, C., Fischer, A., and Grospierre, B. L. (2002). Three Novel Mutations of the CIITA Gene in MHC Class II-Deficient Patients with a Severe Immunodeficiency. *Immunogenetics.* 53:821–829.

Elliot, S. L., Blanford, S., and Thomas, M. B. (2002). Host–Pathogen Interactions in a Varying Environment: Temperature, Behavioural Fever and Fitness. *Proceedings of Royal Society London.* 269: 1599–1607.

Endler, D. (1998). Intrusion detection: Applying Machine Learning to Solaris Audit Data. *Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC"98).* December 07-11. Los Alamitos, CA: 267-279.

Endoh, S., Toma, N., and Yamada, K. (1998). Immune algorithm for n-TSP. *Proceedings of IEEE International Conference on Systems, Man, and Cybernetics*. October 11-14, San Diego, CA. 3844-3849.

Endy, D., and Brent, R. (2001). Modelling Cellular Behaviour. *Nature*. 409: 391-395.

Farmer, J. D., Packard, N. H., and Perelson, A. S. (1986). The Immune System, Adaptation and Machine Learning. *Physica.* D(22): 187-204.

Feng, H., Zeng, Y., Graner, M. W., and Katsanis, E. (2002). Stressed Apoptotic Tumor Cells Stimulate Dendritic Cells and Induce Specific Cytotoxic T Cells. Blood, 100(12): 4108-4115.

Flores, R., Delgado, S., Gas, M. E., Carbonell, A., Molina, D., Selma Gago, Pena, M. D. L. (2004). Viroids: The Minimal Non-Coding RNAs with Autonomous Replication. *FEBS Letters*. 567:42–48.

Forrest, S., Balthrop, J., Glickman, M., and Ackley, D. (2002). Computation in the wild. In: Park, K., and Willins, W. ed. *The internet as a large-complex system.* Oxford University Press.

Forrest, S., and Perelson, A. S. (1992). Computation and the Immune System. *SIGBIO Newsletter, Association for Computing Machinery*. 12(2): 52-57.

Forrest, S., Perelson, A. S., Allen, L., and Cherukuri, R. (1994). Self-nonself Discrimination in a Computer. *Proceedings of IEEE Symposium on Research in Security and Privacy.* May 16-18. Los Alamitos, CA.

Forrest, S., Javornik, B., Smith, R. E., and Perelson, A. S. (1993). Using Genetic Algorithms to Explore Pattern Recognition in the Immune System. *Evolutionary Computation*. 1(3): 191-211.

Forrest, S., Hofmeyr, S., and Somayaji, A. (1997a). Computer immunology. *Communications of the ACM*.

Forrest, S., Somayaji, A., and Ackley, D. (1997b). Building diverse computer systems. In *Proceedings of the 6th workshop on Hot Topics in Operating Systems*, Los Alamitos, CA. IEEE Computer Press.

Forrest, S., Hofmeyr, S. A., Somayaji, A., and Longstaff, T. A. (1996). A Sense of Self for UNIX Processes. *Proceedings of the IEEE Symposium on Security and Privacy.* May 6-8. Los Alamitos, CA: IEEE, 120-128.

Foukia, N., Billard, D., and Harms, P. J. (2001). Computer System Immunity using Mobile Agents. *Proceedings of 8th HP OpenView University Association WS (HPOVUA'2001).* June 24-27. Berlin, Germany.

Garfinkel, T. (2003). Traps and Pitfalls: Practical Problems in System Call Interposition Based Security Tools. *Proceedings of the Internet Society's 2003 Symposium on Network and Distributed System Security.* February 6-7. San Diego, California.

Gasper, A., Collard, P. (1999). From GAs to artificial immune systems: improving adaptation in time dependent optimization. *Proceedings of the Congress on Evolutionary Computation (CEC 99)*. July 10-16. Washington DC. 3:1999 - 1866.

Grimholt, U., Larsen, S., Nordmo, R., Midtlyng, P., Kjoeglum, S., Storset, A., Saebø, S., and Stet, R. J. M. (2003). MHC polymorphism and disease resistance in Atlantic salmon (Salmo salar); facing pathogens with single expressed major histocompatibility class I and class II loci. *Immunogenetics*. 55:210–219.

Gonzalez, F. (2003). *A Study of Artificial Immune Systems Applied to Anomaly Detection.* University of Memphis: Ph.D. Thesis.

Gerald, F. (2002). Forging a New Era in Infectious Disease Research. *Science for Life,* 10-11.

Gabriel, S. B., Schaffner, S. F., Nguyen, H., Moore, J. M., Roy, J., Blumenstiel, B., Higgins, J., De Felice, M., Lochner, A., Faggart, M., Liu-Cordero, S. N., Rotimi, C., Adeyemo, A., Cooper, R., Ward, R., Lander, E. S., Daly, M. J., Altshuler D. (2002). The Structure of Haplotype Blocks in the Human Genome, *Science*. 296:2225-2229.

Gallucci, S., Lolkema, M., and Matzinger, P. (1999). Natural Adjuvants: Endogenous Activators of Dendritic Cells. *Nature Medicine.* 5(11): 1249-1255.

Gannod, G. C., and Cheng, B. H. C. (1999). A Framework for Classifying and Comparing Software Reverse Engineering and Design Recovery Techniques. *Proceedings of Sixth Working Conference on Reverse Engineering,* October 06 – 08. Atlanta,Georgia: IEEE, 77– 88.

Gannod, G. C., Chen, Y., and Cheng, B. H. C. (1998). An Automated Approach for Supporting Software Reuse via Reverse Engineering. *Proceedings of 13th IEEE International Conference on Automated Software Engineering,* October 13-16. Honolulu, HI: 94 – 103.

Germain, R. N. (1995). MHC-Associated Antigen Processing, Presentation, and Recognition Adolescence, Maturity and Beyond. *The Immunologist*. 3/5-6, pp. 185-190

Germain, R. N. (1994). MHC-Dependent Antigen Processing and Peptide Presentation: Providing Ligands for T Lymphocyte Activation. *Cell*. 76: 287-299

Ghosh, A. K., Schwartzbard, A., and Schatz, M. (1999). Learning Program Behavior Profiles for Intrusion Detection. *Proceedings of the Workshop on Intrusion Detection and Network Monitoring.* April 9-12. Santa Clara, California, USA.

Giffin, J. T., Jha, S., and Miller, B. P. (2002). Detecting Manipulated Remote Call Streams. *Proceedings of the 11th USENIX Security Symposium.* August 5-9. San Francisco, USA.

Gibert, C. and Routen, T. (1994). Associative memory in an immune based system. In *Proceedings of AAAI-94.* 2: 852-857. AAAI Press, Menolo Park, California

Goldmann, W. (2003). The Significance of Genetic Control in TSEs. *MicrobiologyToday.* 30/Nov. 03: 170-171.

Goldsby, R. A. (2003). New York : W H Freeman & Company, 2003

Greensmith, J., Aickelin, U., and Cayzer, S. (2005). Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection", *Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS-2005)*

Greten, T. F., and Schneck, J. P. (2002). Development and Use of Multimeric Major Histocompatibility Complex Molecules. *Clinical and Diagnostic Laboratory Immunology*. 9(2): 216–220.

Ham, M. V., Lith, M. V., Lillemeier, B., Tjin, E., Grüneberg, U., Rahman, D., Pastoors, L., Meijgaarden, K. V., Roucard, C., Trowsdale, J., Ottenhoff, T., Pappin, D., and Neefjes, J. (2000). Modulation of the Major Histocompatibility Complex Class II–associated Peptide Repertoire by Human Histocompatibility Leukocyte Antigen (HLA)-DO. *Journal of Experimental Medicine.* 191(7):1127-1136.

Hart, E., and Ross, P. (2003). Improving SOSDM: Inspirations from the Danger Theory. *Proceedings of the 2nd International Conference on Artificial Immune Systems (ICARIS 2003).* September 1-3. Edenburg, UK: Springer LNCS, 194–203.

Hart, E., and Ross, P. (2002). Exploiting the Analogy between Immunology and Sparse Distributed Memories: A System for Clustering Non-stationary Data.

Proceedings of International Conference on Artificial Immune Systems (ICARIS 2002). September 9-11. Canterbury, UK: 49-58.

Hare, B. J., Wyss, D. F., Osburne, M. S., Kern, P. S., Reinherz, E. L., and Wagner, G. (1999). Structure, specificity and CDR mobility of a class II restricted single-chain T-cell receptor. Nature Structural Biology. 6(6): 574-581.

Hart, E. (2002). *Immunology as a Metaphor for Computational Information Processing: Fact or Fiction.* Artificial Intelligence Applications Institute, University of Edinburgh: Ph.D. Thesis.

Haunschild, M. D., Freisleben, B., Wiechert, W., and Takors, R. (2002). Distributed Simulation of Metabolic Networks with Model Variants. *Proceedings of the 16th European Simulation Multiconference: Modelling and Simulation.* June 3-5. Fachhochschule Darmstadt, Darmstadt, Germany: 436-440.

Heeg, K., Sparwasser, T., Lipford, G.B., Häcker, H., Zimmermann, S., Wagner, H. (1998). Bacterial DNA as an Evolutionary Conserved Ligand Signalling Danger of Infection to Immune Cells. *European Journal of Clinical Microbiology and Infectious Disease.* 17:464–469.

Hegde, N. R., and Srikumaran, S. (2000). Reverse Immunogenetic and Polyepitopic Approaches for the Induction of Cell-Mediated Immunity against Bovine Viral Pathogens. *Animal Health Research Reviews.* 1(2): 103–118.

Helmer, G., Wong, J., Honavar, V., and Miller, L. (2002). Automated Discovery of Concise Predictive Rules for Intrusion Detection. *Journal of Systems and Software*. 60(2002): 165-175.

Helmer, G., Wong, J., Honavar, V., and Miller, L. (1999). Automated Discovery of Concise Predictive Rules for Intrusion Detection. *Technical Report TR 99-01*. Department of Computer Science. Iowa State University. Ames, IA.

Hercock, R. G. (2002). Co-operative Agents in Network Defence. *Proceedings of the International Conference on Complex Systems (ICCS2002).* Nashua, NH June 9-14.

Hirsh, H., and Japkowicz, N. (1994). Bootstrap-ping Training-Data Representations for Inductive Learning: A Case Study in Molecular Biology. *Proceedings of the 12th National Conference on Artificial Intelligence.* August 1-4. Seattle, WA: AAAI press, 639-644.

Hofmeyr, S. A. (2000). An Interpretative Introduction to the Immune System. Technical Report. Dept. of Computer Science. University of New Mexico

Hofmeyr, S. A., and Forrest, S. (2000). Architecture for an Artificial Immune System. *Evolutionary Computation Journal.* 8(4): 443-473.

Hofmeyr, S. A., and Forrest, S. (1999). Immunity by Design: An Artificial Immune System. Proceedings of the *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO).* July 13-17, 1999, Orlando, Florida USA: 1289-1296.

Hofmeyr, S. A. (1999). *An Immunological Model of Distributed Detection and Its Application to Computer Security.* University of New Mexico: Ph.D. Thesis.

Hofmeyr, S. A., Forrest, S., and Somayaji, A. (1998). Intrusion Detection Using Sequences of System Calls. *Journal of Computer Security.* 6: 151-180.

Honda, W., Kawashima, S., and Kanehisa, M. (2003). Self-Nonself Discrimination Based on Incompatibility of Amino Acid Sequences of Human and Viruses. *Genome Informatics.* 14: 432 – 433.

Hou, H., Zhu, J., Dozier, J. (2002). Artificial Immunity Using Constraint-Based Detectors. *Proceedings of the 5th IEEE Biannual World Automation Congress (WAC'02)*. June 9-13. Orlando, Florida, USA. 13:239- 244.

Hunt, J. E., Fellows, A. (1996). Introducing an Immune Response into a CBR system for Data Mining. *In BCS ESG'96 Conference and published as Research and Development in Expert Systems XIII. 21.*

Hunt, J., and Cooke, D. (1996). The ISYS Project: An introduction. *Technical Report, IP-REP-02.* University of Wales, Aberystwyth, UK.

Hunt, J. E. and Cooke, D. E. (1996). Learning Using an Artificial Immune System. *Journal of Network and Computer Applications*. 19: 189-212.

Hunt, J. E., Cooke, D. E., and Holstein, H (1995). Case Memory and Retrieval Based on the Immune System. *Proceedings of the First International Conference on Case Based Reasoning.* Weloso, M., and Aamodt, A. ed. *Case-Based Reasoning Research and Development.* LNAI 1010: 205 -216. 1995.

Hasnain, S. E., Begum, R., Ramaiah, K. V. A., Sahdev, S., Shajil, E. M., Taneja, T. K., Mohan, M., Athar, M., Sah, N. K., and Krishnaveni, M. (2003). Host-Pathogen Interactions during Apoptosis. *Journal of Biosciences.* 28(3):349-358.

Ichikawa, S., Ishiguro, A., Watanabe, Y., and Uchikawa, Y. (1998). Moderationism in the Immune System: Gait Acquisition of a Legged Robot Using the Metadynamics Function. *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics.* October 11-14. San Diego. CA.

Iqbal, A., and Maarof, M. A. (2003). A Growing Biological Approach for Intelligent Computing. *Proceedings of the Conference on Intelligent Systems and Robotics (CISAR).* May 20-21. Putrajaya, Malaysia.

Iqbal, A., and Maarof, M. A. (2004). Towards Danger Theory based Artificial APC Model: Novel Metaphor for Danger Susceptible Data Codons, In Proc. of International Conference on Artificial Immune Systems (ICARIS 2004).

Iqbal, A. and Maarof, M. A. (2005). Polymorphism and Danger Susceptibility of System Call DASTONs", *Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS-2005).*

Ishiguro, A., Watanabe, Y., Kondo, T., Shirai, Y., and Uchikawa, Y. (1997). A Robot with a Decentralized Consensus-making Mechanism Based on the Immune System. *Proceedings of the 3rd International Symposium on Autonomous Decentralized Systems ISADS'97.* April 9 - 11, 1997, Berlin, Germany: IEEE, 231-237.

Ishii, K. J., Suzuki, K., Coban, C., Takeshita, F., Itoh, Y., Matoba, H., Kohn, L. D., and Klinman, D. M. (2001). Genomic DNA Released by Dying Cells Induces the Maturation of APCs. *Journal of Immunology*. 167: 2602-2607.

Jackson, J. T., Gunsch, G. H., Claypoole, R. L., Jr., and Lamont, G. B. (2003). Blind Steganography Detection Using a Computational Immune System: A Work in Progress. *International Journal of Digital Evidence*. 4(1).

Jain, K., and Sekar, R. (2000). User-Level Infrastructure for System Call Interposition: A Platform for Intrusion Detection and Confinement. *Proceedings of the ISOC Network and Distributed Security Symposium (NSDD '00).* February 3-4. San Diego, California.

Jones, A., and Li, S. (2001). Temporal Signatures for Intrusion Detection. *Proceedings of the 17th Annual Computer Security Applications Conference.* December 10-14. New Orleans, Louisiana.

Jun, J. H., Lee, D. W., and Sim, K. B. (1999). Realization of Cooperative and Swarm Behavior in Distributed Autonomous Robotic Systems Using Artificial Immune System. *Proceedings of IEEE SMC'99.* 4: 614-619.

Jasuja, H. S. (2002). *The Heat Shock Protein Gp96 – The Immune System's Swiss Army Knife*. PhD Thesis.

Kaers, J., Wheeler, R., and Verrelst, H. (2002). Building a Robust Distributed Artificial Immune System. *Proceedings of the First International Conference on Artificial Immune Systems (ICARIS 2002).* September 9-11. Canterbury, UK: 124-131.

Kalady, M. F., Onaitis, M. W., Padilla, K. M., Emani, S., Tyler, D. S., and Pruitt, S. K. (2002). Enhanced Dendritic Cell Antigen Presentation in RNA-Based Immunotherapy. *Journal of Surgical Research.* 105: 17–24

Kamradt, T. M. D., and Mitchison, N. A. (2001). Tolerance and Autoimmunity. *The New England Journal of Medicine.* 344(9): 655-664.

Keen, N., Staskawicz, B., Mekalanos, J., Ausubel, F., and Cook, R. J. (2000). Pathogens and Hosts: The Dance Is the Same, the Couples Are Different. *Proceedings of National Academy of Science.* 97(16): 8752–8753.

Kemmerer, R.A., and Vigna, G. (2002). Intrusion Detection: A Brief History and Overview. *Computer*. 35(4): 27-30.

Kephart, J. O., Sorkin, G. B. Swimmer, M., and White, S. R. (1997). Blueprint for a Computer Immune System. *Proceedings of Virus Bulletin International Conference*. San Francisco, California. October 1-3.

Kephart, J. O. (1994). A Biologically Inspired Immune System for Computers. *Proceedings of Artificial Life: Fourth International Workshop on the Synthesis and Simulation of Living Systems*. Cambridge, MA. July 6-8.

Kephart, J. O. (1994). A Biologically Inspired Immune System for Computers. In: Brooks. R., and Maes, P. ed. *Artificial Life IV*. Cambridge, MA. MIT Press.

Kephart, J. O., Chess, D. M., and White, S. R. (1993). Computers and Epidemiology. *IEEE Spectrum.* 30(5): 20-26.

Kephart, J. O., Sorkin, G. B., Swimmer, M., and White, S. R. (1997). Blueprint for a Computer Immune System. *Proceedings of Virus Bulletin International Conference*. October 1-3. San Francisco, California.

Kim, J., Wilson, W. O., Aickelin, U., and McLeod, J. (2005). Cooperative Automated worm Response and Detection ImmuNe Algorithm (CARDINAL) inspired by T-cell Immunity and Tolerance", *Proceedings of the 4th International Conference on Artificial Immune Systems (ICARIS-2005).*

Kim, J. (2002). Computers are from Mars, Organisms are from Venus. *IEEE Computer,* 35(7): 25-32.

Kim, J. W. (2002). *Integrating Artificial Immune Algorithms for Intrusion Detection.* University of London: Ph.D. Thesis.

Kim, J. W., and Bentley, P. J. (2001). Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator. *Proceedings the Congress on Evolutionary Computation (CEC-2001).* May 27-30. Seoul, Korea: 1244-1252.

Kim, J., and Bentley, P. (1999). An Artificial Immune Model for Network Intrusion Detection. *Proceedings of 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99).* September 13-19. Aachen, Germany.

Kirchner, J. W., and Roy, B. A. (2002). Evolutionary Implications of Host–Pathogen Specificity: Fitness Consequences of Pathogen Virulence Traits. *Evolutionary Ecology Research*.4: 27–48.

Kirchner, J. W., and Roy, B. A. (2001). Evolutionary Implications of Host-Pathogen Specificity: The Fitness Consequences of Host Life History Traits. *Evolutionary Ecology*. 14: 665-692. [\Host-Pathogen\Selected]

Klein, G. (2004). Cancer, Apoptosis, and Nonimmune Surveillance. *Cell Death and Differentiation*. 11: 13–17.

Kleinstein, S. H., and Seiden, P. E. (2000). Simulating the Immune System. *Computing In Science and Engineering.* July/August 2000: 69-77.

Knight, J. C. (2003). Functional implications of genetic variation in non-coding DNA for disease susceptibility and gene regulation. *Clinical Science*. 104: 493–501. [\Noncoding RNA].

Ko, C., Fink, G., and Levitt, K. (1994). Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring. *Proceedings of Computer Security Applications Conference*. December 5-9. IEEE, 134-144.

Kok, C. C., Croager, E. J., Witt, C. S., Kiers, L., Mastaglia, F. L., Abraham, L. J., and Garlepp, M. J. (1999). Mapping of a Candidate Region for Susceptibility to Inclusion Body Myositis in the Human Major Histocompatibility Complex. *Immunogenetics.* 49: 508–516.

Kolpakov F.A. (2002). BIOUML - Framework For Visual Modeling And Simulation Biological Systems. *Proceedings of International Conference on Bioinformatics of Genome Regulation and Structure (BGRS'2002)*. July 14 – 20. Novosibirsk, Russia.

Kontogiannis, K. (1998). Distributed Objects and Software Application Wrappers: A Vehicle for Software Re-Engineering. *Proceedings of Fifth Working Conference on Reverse Engineering.* October 12-14. Honolulu, Hawaii, USA: IEEE, 254 – 254.

Kosoresow, A. P., and Hofmeyr, S. A. (1997). Intrusion Detection via System Call Traces. *IEEE Software.* 14(5): 35-42.

Kowalczyk, D. W. (2002). Tumors and the Danger Model. *Acta Biochimica Polonica.* 49(2): 295-302.

Kruegel. C. (2002). *Network Alertness - Towards an adaptive, collaborating Intrusion Detection System.* Technical University of Vienna: PhD thesis.

Kunde, R. G., Pandjassarame, K., Tin, W. T., and Shoba, R. (2003). MPID: MHC-Peptide Interaction Database for Sequence-Structure-Function Information on Peptides Binding to MHC Molecules. *Bioinformatics.* 19: 309-310.

Lane, T., and Brodley, C. (1997). An Application of Machine Learning to Anomaly Detection, *Proceedings of the 20th NIST-NCSC National Information Systems Security Conference.* October 7-10. Baltimore, Maryland.

Lee, W., and Xiang, D. (2001). Information-Theoretic Measures for Anomaly Detection.*Proceedings of the 2001 IEEE Symposium on Security and Privacy.* May 13-16. Oakland, California, USA.

Lee, W., and Stolfo, S. (1998). Data Mining Approaches for Intrusion Detection. Proceedings of the 7th USENIX Security Symposium. January 26-29. San Antonio, TX.

Lee, W., Stolfo, S. J., and Chan, P. K. (1997). Learning Patterns from Unix Process Execution Traces for Intrusion Detection. *Proceedings of AAAI97 Workshop on AI Methods in Fraud and Risk Management*, 50-56.

Lei, W., and Hirsbrunner, B. (2002). Immune Meechanism based Computer Security Design. *Proceedingds of International Conference on Machine Learning and Cybernetics.* November 4-5. Beijing, China. IEEE, 4: 1887 –1893.

Leisser, C., Rosenberger, G., Maler, S., Fuhrmann, G., Grusch, M., Strasser, S., Huettenbrenner, S., Fassl, S., Polgar D., Krieger, S., Cerni, C., Warbinek, R. H., de Martin, R., and Krupitza, G. (2004). Subcellular Localisation of Cdc25A Determines Cell Fate. *Cell Death and Differentiation*. 11: 80–89.

Leisser, C., Rosenberger, G., Maler, S., Fuhrmann, G., Grusch, M., Strasser, S., Huettenbrenner, S., Fassl, S., Polgar D., Krieger, S., Cerni, C., Warbinek, R. H.,

de Martin, R., and Krupitza, G. (2004). Expression of the Caspase-8 Gene in Neuroblastoma Cells is regulated through an Essential Interferonsensitive Response Element (ISRE). *Cell Death and Differentiation*. 11: 131–134.

Lemonnier, E. (2001). Guidelines for a Long Term Competitive Intrusion Detection System. *Technical Report.* Defcom Sweden.

Lerner, A. C., and Brent, R. (2000). Using Peptide Aptamers to Analyse Proteomes. *New Technologies for Life Sciences: A Trends Guide.* December 2000: 56-59.

Liao, Y., and Vemuri, V. R., (2002). Using Text Categorization Techniques for Intrusion Detection. *Proceedings of the 11th USENIX Security Symposium.* August 5-9. San Francisco, USA.

Lin, W., Alvarez, S. A., and Ruiz, C. (2002). Efficient Adaptive-Support Association Rule Mining for Recommender Systems. *Data Mining and Knowledge Discovery*. 6(1): 83-105.

Lonardi, S. (2001). *Global Detector of Unusual Words: Design, Implementation, and Application to Pattern Discovery in Bio-sequences.* Perdue University: Ph.D. Thesis.

Lutz, M. A., Gervais, F., Bernstein, A., Hattel, A. L., and Correll, P. H. (2002). STK Receptor Tyrosine Kinase Regulates Susceptibility to Infection with Listeria Monocytogenes. *Infection and Immunity.* 70(1): 416–418.

Majno G and Joris I (1995) Apoptosis, oncosis and necrosis: an overview of cell death. *Am J Pathol*.146:3-15

Majors, D. G. (2003). *Operating System Call Integrity of the Linux Operating System.* University of Missouri-Rolla: Masters Thesis.

Manzella, J., And Mutafelija, B. (1992). Concept Of Re- Engineering Life-Cycle. *Proceedings of the Second International Conference on Systems Integration, ICSI '92.* June 15-18. 566 – 571.

Marceau, C. (2000). Characterizing the behaviour of a Program Using Multiple-Length N-grams. *Proceedings of the 2000 Workshop on New Security Paradigms.* September 19- 21. Cork, Ireland.

Martin, J. B., Irini, A. D., and Darren, R. F. (2002). JenPep: A Database of Quatitative Functional Peptide Data for Immunology. *Bioinformatics*. 18: 434-439.

Martinsohn, J. T., Sousa, A. B., Guethlein, L. A., and Howard, J. C. (1999). The Gene Conversion Hypothesis of MHC Evolution: A Review. *Immunogenetics*. 50: 168–200.

Mastellos, D., Morikis, D., Strey, C., Holland, M. C., and Lambris, J. D. (2004). From atoms to systems: a cross-disciplinary approach to complement-mediated functions. *Molecular Immunology*. 41 (2004):153–164

Mattick, J. S. (2001). Non-coding RNAs: The Architects of Eukaryotic Complexity. *European Molecular Biology Organization Reports*. 21(11):986-991.

Matzinger, P. (2002). The Danger Model: A Renewed Sense of Self. *Science Magazine.* 296: 301-305.

Matzinger, P. (2001a). The Danger Model in Its Historical Context. *Scandinavian Journal of Immunology.* 54: 4-9.

Matzinger, P. (2001b). Introduction to the Series. *Scandinavian Journal of Immunology.* 54: 2-3.

Matzinger, P. (1998). An Innate sense of danger. *Seminars in Immunology*. 10: 399-415.

Matzinger, P. The Real Function of the Immune System. Sited on 17-10-2004. URL:http://cmmg.biosci.wayne.edu/asg/polly.html.

Maxion, R. A., and Tan, K. M. C. (2001). Anomaly Detection in Embedded Systems. *Technical Report CMU-CS-01-157.* School of Computer Science, Canegie Mellon University, Pittsburgh, PA.

Maxion, R. A., and Tan, K. M. C. (2000). Benchmarking Anomaly-Based Detection Systems. *Proceedings of the 1st International Conference on Dependable Systems and Networks.* June 25-28. New York, USA: IEEE, 623-630.

McCoy, D., and Devarajan, V. (1997). Artificial Immune Systems for Aerial Image Segmentation. *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics.* October 13. Orlando, Florida.

Micheal, C. C., and Ghosh, A. (2000). Two State-Based Approaches to Program-Based Anomaly Detection. *Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC'00).* December 11-15. New Orleans, Louisiana. 21-30.

Mihaela L. Oprea (1999), Antibody Repertoires and Pathogen Recognition: The Role of Germline Diversity and Somatic Hypermutation, PhD Thesis, University of New Mexico, Albuquerque, New Mexico.

Monroy, R. (2004). A Process Algebra Model of the Immune System. In: Negoita, M. G., Howlett, R. J., and Jain, L. C. ed. KES 2004, LNCS 3214. Springer-Verlag Heidelberg. 527-33.

Motwani, R., Cohen, E., Datar, M, Fujiware, S., Gionis, A., Indyk, P., Ullman, J., and Yang, C. (2001). Finding interesting associations without support pruning. *IEEE Transactions on Knowledge and Data Engineering (special issue).* 13:64-78.

Mundhada, S., Luthra, R., and Cano, P. (2004). Association of HLA Class I and Class II genes with *bcr-abl* transcripts in leukemia patients with T (9;22) (q34;q11). *BMC Cancer.* 4(25).

Musilek, P., Lau, A., Reformat, M., Scott, L. W. (2005). Immune Programming. Information Science. Elsevier. *In Press*

Nathan, C., and Shiloh, M. U. (2000). Reactive Oxygen and Nitrogen Intermediates in the Relationship between Mammalian Hosts and Microbial Pathogens. *Proceedings of National Academy of Science.* 97(16): 8841–8848.

Narasimhan, P., Kihlstrom, K. P., Moser, L. E., and Smith, P. M. M. (1999). Providing support for survivable CORBA applications with the Immune system. *Proceedings of the 19th IEEE International Conference on Distributed Computing Systems (ICDCS '99).* 31 May – 04 June. Austin, TX: 507 -516.

Norvill, T. (2001). *Auditing and Event Correlation.* University of Queensland: B.E. Hons. Thesis.

Nyeo, S. L., and Yang, I. C., (2002). Codon Distributions In DNA Sequences of Escherichia Coli. *Journal of Biological Systems*. 10(1): 47-60.

Ohno, T., and Nishimura, M. (2004). Detection of a New Cerebral Malaria Susceptibility Locus, Using CBA Mice. *Immunogenetics*.56: 675–678.

Operea, M., and Forrest, S. (1999). How the Immune System Generates Diversity: Pathogen Space Coverage with Random and Evolved Antibody Libraries. *Proceedings of Genetic and Evolutionary Computation Conference (GECCO'99)*. Orlando, Florida. July 13-17.

Paul, W. E. (2003). Fundamental Immunology. Philadelphia, Pa.: Lippincott Williams & Wilkins, 2003

Paula, F.S., Reis, M.A., Fernandes, D.A.M., Geus, P.L. (2002). ADenoIdS: A Hybrid IDS based on the Immune System. Proceedings of *ICONIP2002: 9th International Conference on Neural Information Processing, November* 18-22. Singapura. 3: 1479-1484.

Peretti, M., Villard, J., Barras, E. L., Madeleine Zufferey, M., and Reith, W. (2001). Expression of the Three Human Major Histocompatibility Complex Class II Isotypes Exhibits A Differential Dependence on the Transcription Factor RFXAP. *Molecular and Cellular Biology*. 21(17): 5699–5709.

Pinto, H., Han, J., Pei, J., Wang, K., Chen, Q., and Dayal, U. (2001). Multi-Dimensional Sequential Pattern Mining. *Proceedings of the tenth international conference on Information and knowledge management.* November 5-10. Atlanta, Georgia.

Provos, N. (2002). Improving Host Security with System Call Policies. *CITI Technical Report 02-3.* Center for Information Technology Integration. University of Michigan. Ann Arbor, MI.

Quinnell, R. J., Lorna J. Kennedy, L. J., Barnes, A., Courtenay, O., Dye, C., Garcez, L. M., Marie-Anne Shaw, M. A., Carter, S. D., Thomson, W., and Ollier, W. E. R. (2003). Susceptibility to Visceral Leishmaniasis in the Domestic Dog is Associated with MHC Class II Polymorphism. *Immunogenetics.* 55:23–28.

Ranang, M. T. (2002). *An Artificial Immune System Approach to Preserving Security in Computer Networks.* Norwegian University of Science and Technology: Masters Thesis.

Reisy, M., Paula, F., Fernandes, D., and Geus, P. (2002). A Hybrid IDS Architecture Based on the Immune System. *Proceedings of the Wseg2002: Workshop on Security of Computer Systems.* May 22. Buzios, RJ, Brazil.

Renia, L., Xia, D., Samols, D., and Nussenzweig, V. (1993). Transgenic Mice Expressing C-Reactive Protein are Susceptible to Infection with Plasmodium yoelii Sporozoites. *Infection and Immunity*. 61(1): 348-349.

Rigoutsos, and Floratos, A. (1998). Combinatorial Pattern Discovery in Biological Sequences: The TEIRESIAS Algorithm. *Bioinformatics.* 14(1): 55-67.

Rohrer, M. W. (2000). Seeing is Believing: The Importance of Visualization in Manufacturing Simulation. *Proceedings of the 2000 Winter Simulation Conference (WSC 2000).* December 10-13. Orlando, FL: ACM,1211-1216.

Rooke, R., Waltzinger, C., Benoist, C., and Mathis, D. (1999).Positive Selection of Thymocytes Induced by Gene Transfer: MHC Class II Mediated Selection of CD8 Lineage Cells. *International Immunology*. 11(10):1595-1600.

Roy, S., Hill, A. V. S., Knox, K., Griffithsand, D., Crook, D. (2002). Association of Common Genetic Variant with Susceptibility to Invasive Pneumococcal Disease. *BMJ*. 324:1369.

Sarafijanovic, S., and Boudec, J. Y. L. (2004). An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors. *Proceedings of the 3rd International Conference on Artificial Immune Systems (ICARIS-2004),* pp. 342 – 356.

Sathyanath, S., and Sahin, F. (2002). AISIMAM - An Artificial Immune System Based Intelligent Multi-Agent Model and its Application to a Mine Detection Problem. *Proceedings of the International Conference on Artificial Immune Systems (ICARIS 2002).* September 9-11. Canterbury, UK: 22-31.

Saab, R., Monroy, R., and Godínez, F. (2002). Towards a Model for an Immune System. In: Coello Coello, C. A., de Albornoz, A., Sucar, L. E., and Battistutti, O. C. ed. MICAI 2002, LNCS 2313. Springer-Verlag Heidelberg. 401-410.

Satya, R. V., Mukherjee, A., and Ranga, U. (2003). A Pattern Matching Algorithm for Codon Optimization and CpG Motif-Engineering in DNA Expression Vectors. *Proceedings of the Computational Systems Bioinformatics (CSB'03).* August 11-14. Stanford, CA.

Satya, R. V., Mukherjee, A., and Ranga, U. (2003). Codon Optimization for DNA Vaccines and Gene Therapy Using Pattern Matching. *Proceedings of the Computational Systems Bioinformatics (CSB'03).* August 11-14. Stanford, CA.

Secker, A., Freitas, A. A., and Timmis, J. (2003). A Danger Theory Inspired Approach to Web Mining, *Proceedings of 2nd International Conference on Artificial Immune Systems (ICARIS 2003).* Springer LNCS 2787: 156–167.

Sekar, R., Bendre, M., Dhurjati, D., and Bollineni, P. (2001). A Fast Automaton-Based Method for Detecting Anomalous Program Behaviors. *Proceedings of IEEE Symposium on Security and Privacy.* May 14-16. Oakland, CA.

Sekar, R., and Uppuluri, P. (1999). Synthesizing Fast Intrusion Prevention/Detection Systems from High-Level Specifications. *Technical Report TR99-02.* Department of Computer Science. Iowa State University.

Sekar, R., Bowen, T., and Segal, M. (1999). On Preventing Intrusions by Process Behavior Monitoring. *Proceedings of the Workshop on Intrusion Detection and Network Monitoring.* April 9-12. Santa Clara, California, USA.

Sekar, R., Cai, Y., and Segal, M. (1998). A specification based approach for building survivable systems. *Proceedings of the 1998 National Information Systems Security Conference (NISSC'98).* October 5-8 1998. Arlington, VA: 338-347.

Sercarz, E. E., and Maverakis, E. (2003). MHC-Guided Processing: Binding of Large Antigen Fragments. *Nature Reviews Immunology.* 3:621–629.

Sigal, L. J., Ramirez, M. C., and Soukhanova, A. L. (2001). Mechanisms of MHC Class I Antigen Presentation and Cytotoxic T- Lymphocyte Immunity. *Scientific port*. Fox Chase Cancer Center.

Sioud, M. (2002). How Does Autoimmunity Cause Tumor Regression? A Potential Mechanism Involving Cross-Reaction through Epitope Mimicry. *Molecular Medicine*. 8(3): 115–119.

Sim, R. B., and Tsiftsoglou, S. A. (2004). Proteases of the complement system. Biochemical Society Transactions. 32(1):21-27.

Skormin, V. A., Delgado-Frias, J. G., McGee, D. L., Giordano, J. V., Popyack, L. J., Gorodetski, V. I., and Tarakanov, A. O. (2001). BASIS: A Biological Approach to System Information Security. *Proceedings of International Workshop: Mathematical Methods, Models and Architectures for Computer Network Security.* Springer Verlag, LNCS 2052:127-142.

Smith, D. J. (1997). *The Cross-Reactive Immune Response: Analysis, Modeling, and Application to Vaccine Design.* University of New Mexico: Ph.D. Thesis.

Snoek, M., Albertella, M.R., Kooij, M. V., Wixon, J., Vugt, H. V., Groot, K. D., and Campbell, R. D. (2000). G7c, A Novel Gene in the Mouse and Human Major Histocompatibility Complex Class III Region, Possibly Controlling Lung Tumor Susceptibility. *Immunogenetics*. 51:383–386.

Som, A., Chattopadhyay, S., Chakrabarti, J., and Bandyopadhyay, D. (2001). Codon Distributions in DNA. *arXiv:physics/0102021.* v1.

Somayaji, A. (2002). *Operating System Stability and Security through Process Homeostasis*. University of New Mexico: Ph. D. Thesis.

Somayaji, A., Hofmeyr, S., and Forrest, S. (1998). Principles of a Computer Immune System. *Proceedings of New Security Paradigms Workshop.* September 22-25. Charlottsville, VA: ACM, 75-82.

Spafford, E., and Zamboni, D. (2000). Data Collection Mechanisms for Intrusion Detection Systems. *CERIAS Technical Report 2000-08*. Center for Education and Research in Information Assurance and Security. Purdue University. West Lafayette.

Staskawicz, B. J., Mudgett, M. B., Dangl, J. L., and Galan, J. E. (2001). Common and Contrasting Themes of Plant and Animal Diseases. *Science.* 292:2285-2289.

Stergiou, L., and Hengartner, M. O. (2004). Death and More: DNA Damage Response Pathways in the Nematode C. Elegans. *Cell Death and Differentiation*. 11: 21–28.

Stuckenholz, C., Meller, V. H., and Kuroda, M. I. (2003). Functional Redundancy Within *roX1*, a Noncoding RNA Involved in Dosage Compensation in *Drosophila melanogaster. Genetics*. 164: 1003–1014.

Subhadip, R., Arup, K. C., and Mehran, K. (2003). Effective membrane model of the immunological synapse. *Physical Review Letters*. 19: 208101-1-4.

Sweeney, L. (2003). That's AI? A History and Critique of the Field. *Technical Report, CMU-CS-03-106.* School of Computer Science, Carnegie Mellon University. Pittsburgh Pittsburgh, Pennsylvania, USA.

System Intrusion Analysis and Reporting Environment (SNARE). *Intersect Alliance.* URL: http://www.intersectalliance.com/

Tai, T. S., Fang, L. W., and Lai, M. Z. (2004). c-FLICE Inhibitory Protein Expression Inhibits T-Cell Activation. *Cell Death and Differentiation*. 11: 69–79.

Tavtigian, S. V., et al. (2001). A Candidate Prostate Cancer Susceptibility Gene at Chromosome 17p. *Nature Genetics.* 27:172-180.

Termier, M. (2001). Genome Analysis and Sequences with Random Letter Distribution. *Proceedings of Algorithms Seminar.* April 2. Paris, France: 63-66.

Timmis, J. I. (2001). *Artificial Immune Systems: A Novel Data Analysis Technique Inspired by the Immune Network Theory.* University of Wales, Aberystwyth: PhD Thesis.

Timmis, J. I., Neal, M., and Hunt, J. (1999). Data Analysis with Artificial Immune Systems and Cluster Analysis and Kohonen Networks: Some Comparisons. *Proceedings of IEEE International Conference on Systems, Man and Cybernetics.* October 12-15. Tokyo, Japan: IEEE, 922-927.

Toma, N., Endo, S. & Yamada, K. (1999). Immune Algorithm with Immune Network and MHC for Adaptive Problem Solving. *Proc. of the IEEE System, Man, and Cybernetics*, IV. October 12-15. Tokyo, Japan: IEEE, 271-276.

Toth, T. (2003). *Improving Intrusion Detection Systems.* Technical University of Vienna: Ph.D. thesis.

Udaka, K., Wiesmuller, K. H., Kienle, S., Jung, G., Tmamura, H., Yamagishi, H., Okumura, K., Walden, P., Suto, T., Kawasaki, T. (2000). An Automated Prediction of MHC Class I Binding Peptides based on Positional Scanning with Peptide Libraries. *Immunogenetics*.51: 816-828.

Vaidyanathan, P. P., and Yoon, B. J. (2002). Digital Filters For Gene Prediction Applications. *Proceedings of 36th Asilomar Conference on Signals, Systems, and Computers*. Monterey, CA.

Vallance, B. A., and Finlay, B. B. (2000). Exploitation of Host Cells by enteropathogenic Escherichia Coli. *Proceedings of National Academy of Science.* 97(16): 8799–8806.

Van den Berg, H. A., and Rand, D. A. (2003). Antigen Presentation on MHC Molecules as a Diversity Filter That Enhances Immune Efficacy. *Journal of Theoretical Biology.* 224(2):249-67.

Van den Elsen, P. J., Gobin, S. J. P., van Eggermond, M. C. A. J., and Peijnenburg, A. (1998). Regulation of MHC Class I and II Gene Transcription: Differences and Similarities. Immunogenetics. 48: 208–221.

Van der Wel, N. N., Sugita, M., Fluitsma, D. M., Cao, X., Schreibelt, G., Brenner, M. B., and Peters, P. J. (2003). CD1 and Major Histocompatibility Complex II Molecules Follow a Different Course during Dendritic Cell Maturation. *Molecular Biology of the Cell.* 14: 3378–3388.

Vance, R. E. (2000). Cutting Edge Commentary: A Copernican Revolution? Doubts about the Danger Theory. *The Journal of Immunology.* 165: 1725–1728.

Vodovar, N., Acosta, C., Lemaitre, B., and Boccard, F. (2004). Drosophila: a polyvalent model to decipher host–pathogen interactions. *TRENDS in Microbiology*. 12(5): 235-242.

Wagner, D., and Soto, P. (2002). Mimicry Attacks on Host-Based Intrusion Detection Systems. *Proceedings of the 9th ACM conference on Computer and communications security.* November 18-22. Washingtion, DC, USA: ACM, 255 – 264.

Wagner, D., and Dean, D. (2001). Intrusion Detection via Static Analysis. *Proceedings of the 2001 IEEE Symposium on Security and Privacy.* May 13-16. Oakland, CA.

Walsh, E. C., Mather, K. A., Schaffner, S. F., Farwell, L., Daly, M. J., Patterson, N., Cullen, M., Carrington, M., Bugawan, T. L., Erlich, H., Campbell, J., Barrett, J., Miller, K., Thomson, G., Lander, E. S., and Rioux, J. D. (2003). An Integrated Haplotype Map of the Human Major Histocompatibility Complex. *American Journal of Human Genetics.* 73:580–590.

Wang, J. H., and Reinherz, E. L. (2000). Structural Basis of Cell–Cell Interactions in the Immune System. *Current Opinion in Structural Biology.* 10:656–661.

Wang, K., Yabo, X., Jeffrey, X. Y. (2004). Scalable Sequential Pattern Mining for Biological Sequences. *Proceedings of the Thirteenth ACM conference on Information and knowledge management*. November 8-13. Washington DC, USA.

Wang, K., He, Y., Cheung, D. W. (2001). Mining confident rules without support requirement. *Proceedings of the tenth international conference on Information and knowledge management.* November 5-10. Atlanta, Georgia.

Wang, L., Smith, D., Bot, S., Dellamary, L., Bloom, A., and Bot, A. (2002). Noncoding RNA Danger Motifs Bridge Innate and Adaptive Immunity and are Potent Adjuvants for Vaccination. *Journal of Clinical Investigation.* 110(8): 1175-1184.

Wang, L., and Hirsbrunner, B. (2002). Immune Mechanism Based Computer Security Design. *Proceedings of IEEE International Conference on Machine Learning and Cybernetics.* November 4-5. Beijing, China. 4: 1887 –1893.

Warrender, C., Forrest, S., and Pearlmutter, B. (1999). Detecting Intrusions Using System Calls: Alternative Data Models. *Proceedings of the IEEE Symposium on Security and Privacy.* May 9-2. Oakland, California, USA: IEEE Computer Society, 133-145.

Watanabe, Y., and Ishida, Y. (2003). Mutual Tests among Agents in Distributed Intrusion Detection Systems Using Immunity-Based Diagnosis. *Proceedings of the Eighth International Symposium on Artificial Life and Robotics (AROB 8th '03)*. January 24-26. Beppu Oita Japan. 1: 682-685.

Watanabe, Y., and Ishida, Y. (2002). Fault Detection for Mobile Agent System Using Immunity based Diagnosis. *International Conference on Knowledge-*

Based Intelligent Information and Engineering Systems (KES'2002). September 16-18. Crema, Italy

Watanabe, Y., Ishiguro, A., Shirai, Y., and Uchikawa, Y. (1998). Emergent Construction of Behavior Arbitration Mechanism Based on the Immune System. *Advanced Robotics*. 12(3): 227-242

Watkins, A. B., and Boggess, L. C. (2002). A New Classifier Based On Resource Limited Artificial Immune Systems. *Proceedings of the 2002 Congress on Evolutionary Computation (CEC '02)*. May 12-17. Honolulu, HI. 2: 1546 – 1551.

Watkins, A.B., and Boggess, L. C. (2002). A Resource Limited Artificial Immune Classifier**.** *Proceedings of the 2002 Congress on Evolutionary Computation (CEC'02)*. May 12-17. Honolulu, HI. 1: 926 –931.

Watts, M., Munday, B. L., and Burke, C. M. (2001). Immune responses of teleost fish. *The Australian Veterinary Journal.* 79(8): 570-574.

Weis, J. J. (2002). Host-Pathogen Interactions and the Pathogenesis of Murine Lyme-Disease. Current Opinion in Rheumatology.14:399–403.

Wells, A. D., Rai, S. K., Salvato, M. S., Band, H., and Malkovsky, M. (1998). Hsp72-Mediated Augmentation of MHC Class I Surface Expression and Endogenous Antigen Presentation. *International Immunology*. 10(5):609-617.

Willcox, B. E., Gao, G. F., Wyer, J. R., Ladbury, J. E., Bell, J. I., Bent K. Jakobsen, and van der Merwe, P. A. (1999). TCR Binding to Peptide-MHC Stabilizes a Flexible Recognition Interface. *Immunity*. 10:357–365.

Williamson, M. M. (2002). Biologically Inspired Approaches to Computer Security. *Technical Report, HPL-2002-131.* Information Infrastructure Laboratory. HP Laboratories Bristol.

Williams, P. D., Anchor, K. P., Bebo, J. L., Gunsch, G. H., and Lamont, G. D. (2001). CDIS: Towards a Computer Immune System for Detecting Network Intrusions. *Proceedings of Fourth International Symposium on Recent Advances in Intrusion Detection (RAID 2001).* October 10-12. Davis, CA.

White, S. R., Swimmer, M., Pring, E. J., Arnold, W. C., Chess, D. M., and Morar, J. F. (1999). *Anatomy of a Commercial-Grade Immune System. IBM Research White Paper*.

Wykert, A. K. F., and Miller, J. F. (2003). Hypervirulence and Pathogen Fitness. TRENDS in Microbiology. 11(3): 105-108.

Yahya, H. (2001). *The Miracle of the Immune System.* Goodword Books.

Yanchao, Z., Xirong, Q., Wendong, W., and Shiduan, C. (2001). An immunity-based model for network intrusion detection. *Proceedings of International Conferences on Info-tech and Info-net, Proceedings (ICII 2001)*. Oct. 29 - Nov.1. Beijing. 5: 24 -29.

Zaki, M. J., Parthasarathy, S., Li, W., and Ogihara, M. (1997). Evaluation of Sampling for Data Mining of Association Rules. *Proceedings of the 7th International Workshop on Research Issues in Data Engineering (RIDE '97).* April 7-8. Birmingham, England.

Zamboni, D. (2001). Using Internal Sensors for Computer Intrusion Detection. Purdue University. Ph.D. Thesis.

Zhou, S., Yang, H., Luker, P., and He, X. (1999). A Useful Approach to Developing Reverse Engineering Metrics. *Proceedings of the Twenty-Third Annual International Computer Software and Applications Conference.* October 25 – 26. Phoenix, Arizona: 320 – 321.