Artificial Immune System (AIS) Research in the Last Five Years

D. Dasgupta, Z. Ji
The University of Memphis
Memphis, TN 38152
dasgupta@memphis.edu, zhou.ji@stjude.org

F. González
Universidad Nacional de Colombia
Bogotá, Colombia

Abstract- Immunity-based techniques are gaining popularity in wide area of applications, and emerging as a new branch of Artificial Intelligence (AI). The paper surveys the major works in this field during the last five years, in particular, reviewed the works of existing methods and the new initiatives.

1 Introduction

Various aspects of biology have always been the inspiration in developing computational models and problem solving methods. The immune system is one such system that has recently drawn significant attention; and as a result, the Artificial Immune System (AIS), has emerged. The powerful information processing capabilities of the immune system, such as feature extraction, pattern recognition, learning, memory, and its distributive nature provide rich metaphors for its artificial counterpart.

The immune system, however, is a system with high complexity and is under active research (from the biological point of view), likewise the current AIS works adopted only a few immune mechanisms. Specifically, three immunological principles are primarily used in a piecemeal in AIS methods. These include the immune network theory, the mechanisms of negative selection, and the clonal selection principles.

The first edited volume in AIS (Dasgupta1999a) took into account the initial works (both theory and applications) in this field until 1998. Although the AIS research has been gaining its momentum since then, the changes in the fundamental methodologies have not been dramatic. This paper tries to summarize the works on existing models and development of new ones during the last five-year period (Dasgupta1999b, deCastro1999, 2002c).

2 Immune system metaphors:

2.1 Immune Network Theory

The immune Network theory had been proposed in the mid-seventies (Jerne1974). The hypothesis was that the immune system maintains an idiotypic network of interconnected B cells for antigen recognition. These cells both stimulate and suppress each other in certain ways that lead to the stabilization of the network. Two B cells are connected if the affinities they share exceed a certain threshold, and the strength of the connection is directly proportional to the affinity they share.

2.2 Negative Selection mechanism

The purpose of negative selection is to provide tolerance for self cells. It deals with the immune system's ability to detect unknown antigens while not reacting to the self cells. During the generation of T-cells, receptors are made through a pseudo-random genetic rearrangement process. Then, they undergo a censoring process in the thymus, called the negative selection. There, T-cells that react against self-proteins are destroyed; thus, only those that do not bind to self-proteins are allowed to leave the thymus. These matured T-cells then circulate throughout the body to perform immunological functions and protect the body against foreign antigens.

2.3 The Clonal Selection Principle

The Clonal Selection Principle describes the basic features of an immune response to an antigenic stimulus. It establishes the idea that only those cells that recognize the antigen proliferate, thus being selected against those that do not. The main features of the Clonal Selection Theory are that:

- The new cells are copies of their parents (clone) subjected to a mutation mechanism with high rates (somatic hypermutation);
- Elimination of newly differentiated lymphocytes carrying self-reactive receptors;
- Proliferation and differentiation on contact of mature cells with antigens.

3 Artificial Immune Systems

3.1 Artificial Immune Networks

This method is based on Jerne's idiotypic network theory (Jerne1974), which suggests that the immune system maintains a network of interconnected B-cells. In artificial immune network (AIN) models, a B-cell population is made of two sub-populations: the initial population and the cloned population. The initial set is generated from a subset of raw training data to create the B-cell network. The remainders are used as antigen training items.

Antigens are then selected randomly from the training set and presented to the areas of the B-cell network. If the binding is successful, then the B-cell is

cloned and mutated (Hunt1999). The mutation yields a diverse set of antibodies that can be used in the classification procedure. Once a new B cell is created, an attempt is made to integrate it into the network at the closest B Cells. If the new B cell can not be integrated, it is removed from the population. If no bind is successful, then a B-cell is generated using the antigen as a template and is then incorporated into the network.

An updated version, called AINE (Timmis 2000a, 2001) uses artificial recognition ball (ARB) to represent a number of similar B-cells (not a single B-cell). This resembles the idea of recognition ball in immunology, which refers to the region in the shape space of antigen that an antibody can recognize. It represents a single n-dimensional data item that could be matched by Euclidean distance to an antigen or another ARB. A link between two B-cells is created if the affinity (distance) between two ARBs is below a network affinity threshold (NAT). The results show that the combination of normalizing the stimulation levels of ARBs in the network and the resource allocation mechanism leads to the biasing of AINE towards the strongest pattern in the data set to emerge (Knight2001).

Several enhancements to the AINE model (Timmis 2000b, 2001, Watkin2002a-b) were also suggested including the RLAIS (Resource Limited Artificial Immune system). With the help of ARB concept, other mechanisms in the model are upgraded accordingly. First, the population control is achieved by predefining the total number of B cells that the ARBs represent. In other words, the whole network is resource limited. The ARBs left with no B cells are considered weak and removed from the network. The second improvement is that the results became easier to interpret partly because the confusion of multiple identical B cells does not exist any more. Third, the new model also makes it easy to set the termination condition. RLAIS is, to some degree, analogy of the meta-dynamical behavior observed in the natural immune system to achieve its stability. In the experimental results, periods of stable network size were observed when perturbations of the network size exist.

(Neal2002) designed an approach also based on AINE, called SSAIS (Self-Stabilizing Artificial Immune System). The most important difference from RLAIS is that there is no fixed quantity of resources to be distributed centrally among the ARBs. Though the concept of recourse still exists, but it is dealt locally by ARBs. This work demonstrated the power of decentralization of control mechanism generally used in the fields of genetic algorithm and artificial life.

(Nasaroui2002a) proposed fuzzy ARB, which is represented by a fuzzy set over the domain of discourse consisting of the training data set, as an improvement of the original ARB. Unlike the original AINE model, each fuzzy ARB is allowed to have its own radius of influence and the fuzzy membership function will gradually exclude antigens that are far away from the prototype. The stimulation level is defined by the density of the antigen population around a certain ARB. Some enhancements (Nasaroui2002b-c) are being made to fuzzy AINE in several aspects: avoiding premature convergence, controlling the cloning phase, and controlling population size. Subsequently, (Nasaroui2003) proposed an improvement which appears to be a scalable model powerful enough to deal with real world problems. To represent the temporal nature of the antigen's influence, time is added as an additional dimension to the D-W-B-Cell (Dynamic Weighted B-Cell) in comparison with the classical B cell node defined in antigen space. By allowing stimulation coefficient of each group of D-W-B-cells, which decreases with the age of the subnet, the outdated patterns are removed to control the total population size.

3.2 aiNet

In aiNet (deCastro2000, 2001), the network cells are represented in the same way as in AINE, and a Minimum spanning tree algorithm is used to identify clusters. In aiNet, the input data are assumed to be unlabeled, thus resulting in a kind of competitive learning algorithm. With competitive learning, the clustering of input data is performed such that MSE (mean square error) is iteratively reduced. In aiNet, recognition of an input pattern (antigen) results in cell proliferation, mutation and selection as suggested by the clonal selection theory. A later version of aiNet was developed to solve multimodal function optimization problems (deCastro2002a-c). This algorithm (**CLONAL**G) is based on the clonal selection and affinity maturation principles. It is similar to mutation-based evolutionary algorithms and has several interesting features: 1) population size dynamically adjustable, 2) exploitation and exploration of the search space, 3) location of multiple optima, 4) capability of maintaining local optima solutions, and 5) defined stopping criterion (deCastro2003). A model combining the ideas of aiNet and AINE was also proposed (Wierzchon2002). This work emphasizes its self-organizing ability, i.e. the use of minimal number of control parameters.

The basic implementation issues that are critical to both ANIE and aiNet include the following:

- Data representation.
- Definition of the nodes and edges of the network.
- Network initialization.
- Evaluation of stimulation level and individual influence that contributes to the stimulation level: antigen stimulus, neighbor stimulus and neighbor suppression.
- Effect of stimulation level on the development of the network.
- Criteria to clone a node and determination of clonal rate
- Population control.
- Termination condition.

- Mutation algorithm of the nodes.
- Interpretation of the result network and distinction between training phase and detection phase.
- Choice of various threshold, e.g. to decide when to eliminate network node, when to consider the nodes identical, etc.
- Whether to have more control parameters to make the algorithm more flexible or to have fewer control parameters to make it more self-organizing.

Although many of the issues have been dealt with in the various variations of AINE and aiNet, there remains many open questions, such as scalability, self-organizing ability, robustness to noise, and continual learning ability for dynamic data, etc.

3.3 The Negative Selection Algorithm

Forrest (Forrest1994) proposed the *negative selection* algorithm **(N**SA), which is inspired by the mechanism used by the immune system to train the T-cells to recognize antigens (non-self) and to prevent them from recognizing the body's own cells (self). The idea is to generate a set of (binary) detectors by first randomly making candidates and then discarding those that recognize training self-data. These detectors can later be used to detect anomaly. So the NSA consists of three phases: defining self, generating detectors and monitoring the occurrence of anomalies. Different variations of this algorithm (detector generating schemes) have been proposed. The primary applications of NSA have been in the field of change (or anomaly) detection, where the detectors are generated in the complement space which can detect changes in data patterns. The main component of NS is the choice of a matching rule, which determines the similarity between two patterns in order to classify self/non-self (normal/abnormal) samples. The time complexity of generating detectors is linear with respect to the size of self-data. An estimate for the size of the detector set is needed to ensure a certain level of reliability in detecting anomaly. With larger matching threshold, the generated detectors become sensitive to any anomaly in the data patterns, so more detectors are necessary to achieve a desired level of overall reliability. On the other hand, if the threshold is too small, it may not be possible to generate a reasonable sized detector set from the available self. This suggests that the value of threshold can be used to tune the reliability of detection against the risk of false positives. It was applied to the change-detection in a general case.

Ayara (Ayara2002) reviewed and compared five detector generation schemes of (binary) negative selection algorithms: exhaustive, linear, greedy, binary template, and NSMutation. The last scheme is a modified version of exhaustive algorithm, which introduced somatic hypermutation and elimination of redundancy to exhaustive NS algorithm for better performance.

Gonzalez et al. (Gonzalez2003a) analyzed and compared different binary matching rules in negative selection: r-contiguous matching, r-chunk matching, Hamming distance matching, and its variation Rogers and Tanimoto (R&T) matching. It thus provides a guideline for selecting different matching rules for any negative selection algorithms.

Different representation schemes for the negative selection and detector generation algorithms for such representations have also been explored (Gonzalez 2003b). In particular, representations that are studied include hyper-rectangles (which can be interpreted as rules), fuzzy rules, and hyper-spheres. Four different detector generation algorithms are proposed, accordingly: Negative Selection with Detection Rules (NSDR, an evolutionary algorithm to generate hypercube detectors), Negative Selection with Fuzzy Detection Rules (NSFDR, an evolutionary algorithm to generate fuzzy-rule detectors), Real-valued Negative Selection (RNS, a heuristic algorithm to generate hyper-spherical detectors), and Randomized Real-valued Negative Selection (RRNS, an algorithm for generating hyper-spherical detectors based on Monte Carlo methods). Also, a hybrid immune learning algorithm, which combines RNS (or RRNS) and classification algorithms is developed.

Chao et al. (Chao2002) indicated that information filtering can be possible using the negative selection strategy. This work discussed (1) enhancement so that the information supposed to be kept for special reasons would be safe; (2) life time of the active immune cells or detectors; (3) the effect of history or the order of exposure to different cases; (4) when and how to use group IIS (information immune system).

Another variation of the negative selection model introduces dynamic clonal selection algorithm (DynamiCS) to deal with non-self detection problem in a continuously changing environment (Kim2002a-b). In particular, DynamiCS is based on Hofmeyr's (Hofmeyr2000) idea of dynamics of three different populations: immature, mature, and memory detector populations. Initial immature detectors are generated with random genotypes. Using the negative selection, new immature detectors are added to keep the total number of detectors constant after a predefined number of generations (polarization period T). If a detector is within its predefined life span *L*, and the match counts are larger than a predefined activation threshold *A*, it becomes a memory detector. Mature detectors are used to identify unknown attacks. However, a human security officer's confirmation (co-stimulation) is necessary, which makes the approach dependent on human interaction.

4 Other varieties of AIS models

Hybrid architecture is studied by Grilo (Grilo1999), which includes three major components: cellular

automata, artificial life, and artificial immune systems. The results showed complex and emergent behavior due to the interaction of the immune system agents. While this work is more of a simulation of Complex Adaptive System (CAS) than a problem solving paradigm, the inclusion of cellular automation and artificial life concepts appear to be interesting.

Tarakanov (Tarakanov2000) performed some theoretical studies and proposed a formal mathematical model, called FIS (formal immune system), moreover, the hardware implementation of this model is also under investigation (Tarakanov2002).

Another AIS model that dealt with the problem of scalability and dynamic data is proposed by Hart (Hart2002). This work used a combination of immunological memory and SDM (sparse distributed memories) by embodying the important principles of both types of memory. The algorithm is called SOSDM (Self-Organized SDM). An SDM is composed of a set of physical or hard locations, each of which recognizes data within a specified distance. This method of storing data makes it an ideal candidate for addressing clustering problems in large database.

Recently, a new algorithm, called MILA (Multilevel Immune Learning Algorithm) is proposed (Dasgupta2003). The novelty of this approach is two-folded: (1) more mechanisms of the immune system are utilized, including T helper cells, T suppressor, B Cells, APCs (antigen-presenting cells). This made it quite different from other models, which used only one concept (either B cells or T cells). (2) This algorithm detects in a multilevel, multi-resolution fashion, making large space to explore efficiently for anomaly detection applications.

5 Applications

The role of the immune system may be considered analogous to that of computer security systems (Forrest1994). Long-term research projects have been established in order to build a computer immune system (Dasgupta1999d)(Hofmeyr2000)(Williams 1999) which could augment a simple computer security system with much more. Host based intrusion detection methods construct a database that catalogues the normal behavior over time in terms of the system calls made etc. As this record builds up, the database may be monitored for any system calls not found in the normal behavior database. The authors argue that while simplistic, this approach is not computationally expensive and can be easily used in real time. It also has the advantage of being platform and software independent. An alternative method is the network based intrusion detection approach. This tackles the issue of protecting networks of computers rather than an individual computer. This is achieved in a similar way in monitoring network services, traffic and user behavior and attempts to detect misuse or intrusion by observing departures from normal behavior.

The AIS methods are used in genetic algorithm based design and optimization (Hajela1996, 1999). This approach is applied to some structural optimization problems with two objectives (a two-bar truss structure, a simply supported I-beam, and a 10-bar truss structure). The best designs according to this value are defined as antigens and the rest of the population as a pool of antibodies. The simulation of the immune system is then done as in the previous work of the authors where the technique is used to handle constraints. This approach uses a linear aggregating function to combine objective function and constraint information into a scalar value that is used as the fitness function of a GA (Hajela1999). The use of different weights allows converging to a certain (pre-specified) number of points of the Pareto front, since they make mpt to use any specific technique to preserve diversity. Besides the limited spread of non-dominated solutions produced by the approach, it is well-known that linear aggregating functions have severe limitations for solving multiobjective problems (the mai .

dominatlimlopanti

Despite the initial success of AIS techniques, there remain many open issues. As the field is relatively new, most of the existing works have been exploratory, and the algorithms do not scale. Among others, the following are some aspects that need to be addressed in order to make AISs as useful problem solving technique:

- Improvement of the efficiency of the algorithms.
- Enhancement of the representation.
- Introduction of other mechanisms as necessary
- Development of a unified architecture that can integrate several AIS models.

Tables 1 show a chronological list of some AIS models and techniques that are found in the literature. The table includes a short description of each model or technique, use of specific immunological mechanisms, type of representations, and the intended applications.

Table 1: A time-line of AIS works (1999-2003).

Reference	**Model or technique description**	**Aspects of the BIS modeled**	**Type of representation used**	**Applications**
(Hunt1999)	A machine learning system (Jisys) based on immune networks	Ag-Ab binding. Immune network.	Mixed numerical, categorical and string data.	Fraud detection, Learning.
(Dasgupta1999d)	An architecture for an agent-based intrusion/anomaly detection and response system	Distributed control, Self/non-self discrimination.	Java objects	Computer security.
(Dasgupta1999e)	Combines immune system ideas and genetic algorithms to interpret chemical spectra	Ag-Ab binding. Self/non-self discrimination.	Binary strings	Chemical spectrum recognition.
(Williams1999)	A multi-agent computational immune system (CDIS) for intrusion detection	Ag-Ab binding. Self/non-self discrimination.	Strings from a finite alphabet.	Computer security
(Tarakanov2000)	A formal model of the immune system.	Ag-Ab binding.	Real-valued vectors.	BIS modeling.
(Timmis 2000b)	A resource limited artificial immune system **(RAIN**E) for data analysis that extends the work of Cooke and Hunt [23].	Ag-Ab binding, Immune network.	Real-valued vectors.	Data analysis, Clustering.
(DeCastro2000)	A system based on clonal selection and affinity maturation **(CLONAL**G) for pattern matching and optimization.	Ag-Ab binding. Clonal selection. Affinity maturation.	Binary and integer strings.	Pattern matching, Optimization.
(DeCastro2001a)	An immune network learning algorithm **(aiNe**t).	Ag-Ab binding, Clonal selection, Affinity maturation, Immune network.	Real-valued vectors.	Data analysis, Clustering.
(Hofmeyr2000)	An architecture for an artificial immune system **(Lisy**s) for computer security.	Ag-Ab binding. Self/non-self discrimination, Affinity maturation.	Binary strings.	Computer security.
(Bradley2000)	A machine fault tolerance mechanism based on immune system ideas **(Immunotronic**s).	Self/non-self discrimination.	Binary strings.	Hardware fault detection and tolerance.

(DeCastro2001b)	A simulated annealing algorithm based on the immune systems **(SAN**D) applied to neural network initialization.	Ag-Ab binding, Immune diversity.	Real-valued vectors.	Initialization of feed-forward neural network weights.
(Tarakanov20002)	Architecture to build chips that implement the immune system model proposed	Ag-Ab binding, Immune network.	Real-valued vectors (internally represented as bits).	Pattern matching.
(Nasraoui2002a)	An immune network based algorithm that uses fuzzy theory to model the Ag-Ab matching.	Ag-Ab binding, Immune network.	Real-valued vectors.	Clustering, Web data mining
(Hart2002)	A system to cluster non-stationary data **(SOSD**M) that combines ideas from BIS and sparse distributed memories.	Ag-Ab binding, Immune memory.	Binary strings.	Associative memory, Clustering.
(Coello2002)	An approach to handle constraints in GA based optimization.	Ag-Ab binding, Gene libraries.	Binary strings	Optimization.
(Kim2002a)	An algorithm to perform dynamic learning on changing environments.	Ag-Ab binding, Clonal selection, Self/non-self discrimination.	Binary strings.	Dynamic learning.
(Nasraoui2002a, 2003)	A scalable artificial immune system model for dynamic unsupervised learning based on immune network theory.	Ag-Ab binding, Immune network.	Real-valued vectors.	Clustering, dynamic learning.
(Dasgupta2003)	Multi-Level Immune Learning Algorithm (MILA) combines several immunological features.	Negative selection, Clonal selection, APC	Different representations and matching rules, repertoire optimization	Anomaly detection, pattern recognition

Bibliography

- (Dasgupta1999a), Dipankar Dasgupta, Artificial Immune System and Their Applications, Springer-Verlag, 1999
- (Dasgupta1999b), Dipankar Dasgupta, An overview of artificial immune systems and their applications, Artificial Immune System and Their Applications, 1999
- (Dasgupta1999c), Dipankar Dasgupta and Stephanie Forrest, An anomaly detection algorithm inspired by the immune system, Artificial Immune System and Their Applications, 1999
- (Dasgupta1999d), D. Dasgupta, Immune-based intrusion detection system: a general framework, in *Proceedings of the 22nd national information systems security conferencfe (NISSC), 1999*
- (deCastro1999), L. N. de Castro, F. J. von Zuben, Artificial Immune Systems: Part I - Basic Theory and Applications, Technical Report TR-DCA 01/99, 1999
- (Forrest1994), S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri. Self-Nonself Discrimination in a Computer. In Proceedings of *IEEE Symposium on Research in Security and Privac*y, pages202--212, Oakland, May 16-18 1994.

- (Grilo1999), Antonio Grilo, Artur Caetano, Agostinho Rosa, Immune System Simulation through a Complex Adaptive System Model, Proceeding of the 3rd Workshop on Genetic Algorithms and Artificial Life, 1999
- (Jerne1974), N. K. Jerne, Towards a network theory of the immune system. *Ann. Immunol, (Inst. Pasteur)*, 125C, pp373-389, 1974.
- (Hunt1999), J. Hunt, J. Timmis, D. Cooke, M. Neal and C. King, Jisys: The Development of an Artificial Immune System for Real World Applications, in Artificial Immune System and Their Applications, 1999
- (Kumar1999), Kalmanje KrishnaKumar and James Neidhoefer, Immunized Adaptive Critic for an Autonomous Aircraft Control Application, Artificial Immune System and Their Applications, 1999
- (Williams1999) P. D. Williams, K. P. Anchor, J. L. Bebo, G. H. Gunsh, and G. D. Lamont, CDIS: Towards a computer immune system for detecting network intrusions, Lecture notes in Computer Science, vol. 2212, pp. 117-133, 2001
- (Bradley2000) D. Bradley and A. Tyrell, Immunotronics: Hardware fault tolerance inspired by the immune system, in *Proceedings of the 3rd `International conference on Evoluable Systems (ICES2000)*, vol. 1801, Springer-verlag, Inc., 2000
- (deCastro2000) L. N. de Castro and F. J. V. Zuben, The clone selection algorithm with engineering applications, in *Proceedings of GECCO ' 00, 2000*
- (Hofmeyr2000) S. Hofmeyr and S. Forrest, Architecture for an artificial immune system, Evolutionary Compuiation, vol. 8, no. 4, pp. 443-473, 2000
- (Tarakanov2000), Alexander Tarakanov, Dipankar Dasgupta, A formal model of an artificial immune system, BioSystem, 2000
- (Timmis2000a), Jon Timmis, Mark Neal, John Hunt, An Artificial Immune System for Data Analysis, Biosystems, 2000
- (Timmis2000b), Jon I. Timmis, Artificial Immune Systems: A Novel Data Analysis Technique Inspired by the Immune Network Theory, Dissertation, University of Wales, 2000
- (deCastro2001), Leandro Nunes de Castro & Fernando Jose Von Zuben, aiNet: An Aritificial Immune Network for Data Analysis, in Data Mining: A Heuristic Approach, 2001
- (Knight2001), T Knight and J Timmis, Aine: An immunological approach to data mining, IEEE International Conference on Data Mining, 2001
- (Timmis2001), Jon Timmis and Mark Neal, A resource limited artificial immune system for data analysis, Knowledge Based System, 2001
- (Ayara2002), M. Ayara, J. Timmis, R. de Lemos, L. de Castro and R. Duncan, Negative Selection: How to Generate Detectors, 1st ICARIS, 2002
- (Chao2002), D. Chao and S. Forrest, Information Immune Systems, 1st ICARIS, 2002
- (Coello2002) C. A. Coello and N. Cruz Cores, A parallel implementation of the artificial immune system to handle constraints in genetic algorithms: preliminary results, in *Proceedings of the 2002 Congress on Evolutionary Computation CEC2002, Honolulu, 2002*.
- (deCastro2002a), Leandro N. de Castro & Jon Timmis, An Artificial Immune Network for Multimodal Function Optimization, WCCI 2002, 2002
- (deCastro2002b), L. N. de Castro, J. I. Timmis, Artificial Immune Systems: A Novel Paradigm to Pattern Recognition, in *Artificial Neural Network in Pattern Recognition*, University of Paisley, UK, 2002
- (deCastro2002c), L. N. de Castro and J. Timmis, Hierarchy and Convergence of Immune Networks: Basic Ideas and Preliminary Results, 1st ICARIS, 2002
- (deCastro2002d), Leandro N. de Castro and Jonathan Timmis, Artificial Immune System: A New Computational Intelligence Approach, Springer-Verlag, 2002
- (Gonzalez2002), Fabio Gonzalez, Dipankar Dasgupta, An Immunogenetic Approach to Intrusion Detection, GECCO, 2002
- (Hart2002), E. Hart and P Ross, Exploiting the analogy between immunology and Spare Distributed Memories: A System for Clustering Non-stationary data, 1st ICARIS, 2002
- (Kim2002a) J. Kim amd P. J. Bentley, Toward an artificial immune system system for network intrusion detection: An investigation of dynamic clonal selection, in *Proceedings of the 2002 Congress on Evolutionary Computation CEC2002*. Honolulu, 2002
- (Kim2002b), J. Kim and P. Bentley, Immune Memory in the Dynamic Clonal Selection Algorithm, 1st ICARIS, 2002
- (Knight2002), T. Knight and J. Timmis, A multi-Layered Immune Inspired Approach to Data Mining, Proceedings of the 4th International Conference on Recent Advances in Soft Computing, 2002
- (Nasaroui2002a), O. Nasaroui, F. Gonzalez and D Dasgupta, The Fuzzy AIS: Motivations, Basic Concepts, and Applications to Clustering and Web Profiling, IEEE International Conference on Fizzy Systems, 2002
- (Nasaroui2002b), Olfa Nasaroui, Dipankar Dasgupta, Fabio Gonzalez, The Promise and Challenges of Artificial Immune Systems Based Web Usage Mining: Preliminary Results, Workshop on Web Analytics at Second SIAM International Conference on Data Mining (SDM), 2002
- (Nasaroui2002c), Olfa Nasaroui, Dipankar Dasgupta, Fabio Gonzalez, A Novel Artificial Immune System Approach to Robust Data Mining, GECCO, 2002
- (Neal2002), M. Neal, An Artificial Immune System for Continuous Analysis of Time-Varying Data, 1st ICARIS, 2002
- (Watkins2002a), A. B. Watkins and L. C. Boggess, A Resource Limited Artificial Immune Classifier, IEEE World Congress on Computational Intelligence, 2002

- (Watkins2002b), Watkins and Timmis, Artificial Immune Recognition System (AIRS): Revisions and Refinements, 1st ICARIS, 2002
- (Wierzchon2002), Wierzchon and U. Kuzelewska, Stable Clusters Formation in an Artificial Immune Systems, 1st ICARIS, 2002
- (Cao2003), Y. Cao and D. Dasgupta, An Immunogenetic Approach in Chemical Spectrum Recognition, in Advances in Evolutionary Computing, Springer-Verlag, 2003.
- (Dasgupta2003), Dipankar Dasgupta, Senhua Yu, Nivedita Sumi Majumdar, MILA - Multilevel Immune Learning Algorithm, In the proceedings of GECCO, July 2003
- (deCastro2003), L. N. de Castro, J. I. Timmis, Artificial Immune Systems as a Novel Soft Computing Paradigm, Soft Computing Journal, 2003
- (Gonzalez2003a), Fabio Gonzalez, Dipankar Dasgupta, and Jonatan Gomez, The Effect of Binary Rules in Negative Selection, GECCO-2003, 2003
- (Gonzalez2003b), Fabio Gonzalez, Dipankar Dasgupta, and Luis Fernando Nino, A Randomized Real-Value Negative Selection Algorithm, ICARIS-2003, 2003
- (Kumar2003), K. KrishnaKumar, Artificial Immune System Approaches for Aerospace Application, 41st Aerospace Sciences Meeting & Exhibit, 2003
- (Tarakanov2002) A. Tarakanov and D. Dasgupta, An immunochip archtecture and its emulation, in 2002 NASA/DoD Conference on Evoluable Hardware, 2002
- (Narasoui2003) O. Narasoui, F. Gonzalez, C. Cardona, C. Rojas, and D. Dasgupta, A Scalable Artificial Immune System Model for Dynamic Unsupervised Learning, GECCO, 2003
- (Neal2003), Mark Neal, Meta-Stable Memory in an Artificial Immune Network, 2nd ICARIS, 2003
- (Hajela1996), P. Hajela and J. Lee. Constrained Genetic Search via Schema Adaptation. An Immune Network Solution. *Structural Optimizatio*n, 12:11–15, 1996.
- (Hajela1999), J. Yoo and P. Hajela. Immune network simulations in multicriterion design. *Structural Optimizatio*n, 18:85–94, 1999.
- (Singh2001), S. P. N. Singh, and Scott M. Thayer. Immunology Directed Methods for Distributed Robotics: A novel, Immunity –Based Architecture for Robust Control & Coordination. Proceedings of SPIE: Mobile Robots XVI, vol.4573, November 2001.