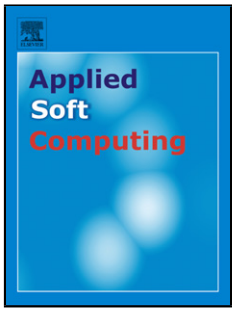
Accepted Manuscript



Title: Recent Advances in Artificial Immune Systems: Models and Applications

Authors: Dipankar Dasgupta, Senhua Yu, Fernando Nino

PII: S1568-4946(10)00272-3
DOI: doi:10.1016/j.asoc.2010.08.024
Reference: ASOC 992

To appear in: *Applied Soft Computing*

Received date: 4-2-2010
Revised date: 13-8-2010
Accepted date: 25-8-2010

Please cite this article as: D. Dasgupta, S. Yu, F. Nino, Recent Advances in Artificial Immune Systems: Models and Applications, *Applied Soft Computing Journal* (2010), doi:10.1016/j.asoc.2010.08.024

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Recent Advances in Artificial Immune Systems: Models and Applications

Dipankar Dasgupta[a], Senhua Yu[a], and Fernando Nino[b]

[a] Department of Computer Science, University of Memphis, USA
[b] Department of Computer Science Dept, National University of Colombia, Colombia

Abstract

The immune system is a remarkable information processing and self learning system that offers inspiration to build Artificial Immune Systems (AIS). The field of AIS has obtained a significant degree of success as a branch of Computational Intelligence since it emerged in the 1990s. This paper surveys the major works in the AIS field, in particular, it explores up-to-date advances in applied AIS during the last few years. This survey has revealed that recent research is centered on four major AIS algorithms: 1) Negative Selection Algorithm; 2) Artificial Immune Networks; 3) Clonal Selection Algorithm; 4) Danger Theory and Dendritic Cell Algorithms. However, other aspects of the biological immune system are motivating computer scientists and engineers to develop new models and problem solving methods. Though an extensive amount of AIS applications has been developed, the success of these applications is still limited by the lack of any exemplars that really stand out as killer AIS applications.

Key words: AIS, review, models, applications

1. History of Artificial immune systems in brief

Artificial Immune System is an area of research that bridges the disciplines of immunology, computer science and engineering [1-3]. Researches on AISs can be divided into immune modeling, theoretical AISs and applied AISs. Research work on applied AIS ranges from developing immune-inspired algorithms, building immune-inspired computer systems, to apply AISs to diverse real world applications. In contrast, immune modeling includes research work detailing models and simulations of natural and artificial immune systems, while theoretical AISs aim at describing the theoretical aspects of AISs, including mathematical modeling of algorithms, convergence analysis, and performance and complexity analysis of such algorithms. This survey mainly covers recent development on applied AISs because it is not only the most vibrant and active branch in the area of AIS but also the research area our group centers on. The most recent and comprehensive survey on theoretical AISs is possibly from that of Timmis et al. [4]. However, an up-to-date relatively comprehensive review on Immune Modeling has not been seen in the literature.

In the last decade, the immune system has drawn significant attention as a potential source of inspiration for novel approaches to solving complex computational problems. Its highly distributed, adaptive, and self-organizing nature, together with its learning, memory, feature extraction, and pattern recognition features offer rich metaphors for its

Accepted Manuscript

ACCEPTED MANUSCRIPT

artificial counterpart. Unlike other engineered systems, AISs require both immunology and engineering to learn from each other through working in an interdisciplinary manner [5]. A collaborative effort of several interdisciplinary research scientists has produced a prolific amount of immune inspired algorithms by extracting or gleaning useful mechanisms from the immune system theories, processes and elements.

In 1994, Forrest et al. [6] published a seminal paper titled "*Self-Nonself Discrimination in a Computer*". They proposed a method called *negative selection algorithm* for distinguishing self from other, which is based on the generation of T cells in the immune system. This method was then applied to the problem of computer virus detection. Since this paper was published, negative selection algorithm has attracted the attention of many researchers and practitioners and has been applied in numerous real world applications. Although a diverse family of negative selection algorithms has been developed, the essential characteristics of the original negative selection algorithm introduced in this paper still remain.

Artificial immune networks (AINs) are other successful models in AISs. Inspired by Farmer et al.'s immune network model [7], the first immune network algorithm was proposed by Ishida [8]. Timmis et al. [9] re-defined and re-implemented the artificial immune network. These works were formally named AINE (Artificial Immune NEtwork) in [10]. An artificial immune network (AIN/AINE) consists of a set of B cells, links between those B cells, which undergo some cloning and mutation operations. This work has been widely used in areas such as data mining and machine learning.

In 2000, De Castro et al. [11] proposed the *clonal selection algorithm* (CSA), later known as CLONALG. CLONALG is based on clonal selection and affinity maturation principles [12]. One cell generation in this algorithm includes the initiation of candidate solutions, selection, clone, mutation, reselection, and population replacement, which are somehow similar to a genetic algorithm (GA). The comparison done in this paper showed that the clonal selection algorithm can reach a diverse set of local optima solutions, while all candidate solutions in the GA converge to the best solution. Through its applications to binary character recognition, multi-modal optimization, and the Traveling Salesman Problem (TSP), this paper also concluded that the algorithm has the capability of performing learning and maintenance of high quality memory.

Several other areas of immunology have recently been reported in the literature to inspire the development of algorithms and computational tools, for example, humoral immune response [13], Danger Theory [14], dendritic cell functions [15], and pattern recognition receptor model [16]. However, these new areas are still immature and under continuous investigation and development. Also, though undeniably, there have been a lot of successful applications of AIS, there are still very few exemplars that really stand out as instances of AISs being used in earnest in industry.

In the last two decades, the AIS community has produced a diverse set of immune inspired algorithms to solve various computational problems or tackle real world applications. An extensive body of literature has been produced in this field, including

Accepted Manuscript

ACCEPTED MANUSCRIPT

AIS textbooks and a wide ranging collection of successful application papers [17]. The first volume in AIS titled "*Artificial Immune Systems and Their applications*" was edited by D. Dasgupta in 1999 [18]. This volume provided an overview of the immune system from the computational viewpoint and took into account the major works in this field until 1998, including the computational models of the immune system and their applications. Subsequently, L. De Castro and J. Timmis [3] wrote the book titled "*Artificial Immune Systems: A New Computational Intelligence Approach*" in 2002. This book provided an accessible introduction to the biological principles of the natural immune system as well as a comprehensive presentation of the AIS basic algorithms; it also preformed a comparative analysis of the immune system and other biological systems and processes. In 2003, Alexander et al. [19] published their book "*Immunocomputing: Principles and Applications*". This book deals mainly with the following: 1) Introduction of immunocomputing; 2) The mathematical basis of the immunocomputing; 3) Various applications of Immunocomputing. This book is the first attempt to introduce and summarize the earlier works in the area of theoretical AIS. Also, In [20] a summary of the research in the AIS was reported On the other hand, a book by Ishida [21] was the first book devoted to presenting immune network models. This book explored the self-organizing network inspired from Jerne's idiotypic network and presented an application of sensor networks using self-organizing networks.

Most recently, D. Dasgupta and. L.F. Nino's book [22] "*Immunological Computation: Theory and Applications*" provided an overview of fundamental immunology concepts and some theoretical models of immune processes. It also presents up-to-date immunology-based computational techniques that are developed in their own research group and other groups worldwide. For instance, real-valued negative selection algorithm, Danger Theory, modeling the germinal centers, and the Multilevel Immune Learning Algorithm (MILA) are discussed. In addition, up to date advances in the AIS are presented and an extensive review on data representations, affinity measures, matching rules, and general abstractions of some immune elements and processes that are used in most immune-based models are included.

International Conferences on Artificial Immune Systems (ICARIS), the flagship conference dedicated entirely to the field of AIS and the major annual activity in the AIS community, have been held yearly since 2002. This conference provides a great opportunity for presenting and disseminating the latest work in the field in AISs. Also, work on AISs often appears in other international conferences, such as the Genetic and Evolutionary Computation Conference (GECCO), the IEEE Congress on Evolutionary Computation, the IEEE World Congress on Computational Intelligence (WCCI), and the International Conference on Artificial Intelligence and Soft Computing (ICAISC).

2. Recent Developments in AIS

While many other areas of the vertebrate immune systems are inspiring computer scientists and engineers to develop new algorithms, four major AIS algorithms have been constantly developed and gained popularity: 1) Negative Selection Algorithms (NSA); 2) Artificial Immune Networks (AINE); 3) Clonal Selection Algorithms (CLONALG). 4)

Accepted Manuscript

ACCEPTED MANUSCRIPT

The Danger Theory and Dendritic Cell Algorithms (DCA). Also, there have been many successful applications of AISs, such as computer security, optimization, data mining, and anomaly detection, etc. Several authors have surveyed and evaluated the filed of AIS from different aspects. For example, Garrett [23] tracked the development of AIS before 2005 followed by attempting to make an assessment of the usefulness of the AIS in terms of “distinctiveness” and “effectiveness”. [24] provided an introduction and analysis of the key developments in AIS within the filed of intrusion detection. Hart and Jimmis [25] discussed the application areas of the AIS and attempted to suggest a set of problem features for the potential applications of AIS. [26] reviewed the state-of-the-art in immunity-based multiobjective optimization algorithms and summarized the real world applications of these algorithms in the reviewed literature. This section surveys the up-to-date advances in the entire area of AIS during recent years. It covers various AIS models and different types of AIS applications, in particular, the most recent advances in this area since 2006. We believe that this work would be an important complement to [4, 23-25], where either the different aspects of the AIS field were surveyed or the recent advances in the AIS field have not been covered. Table 1 summarizes the main AIS algorithms, including the sections where they are presented in this survey and a list of recent references. Among various mechanisms in the complex immune system that have been explored for AIS, self/nonself discrimination was one of the earlier mechanisms identified as a useful metaphor for computation and recently given continued attention. Table 2 summarizes the AIS algorithms inspired by the immune theory of self/non-self discrimination.

Table 1: Summary of immune algorithms and recent references

Models	**Section**	**References**
Negative Selection	Section 2.1.1	[27] [28] [29] [30] [31, 32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53]
Immune Networks	Section 2.1.2	[54] [55] [56] [57] [58] [59] [60, 61] [62] [63]
Clonal Selection	Section 2.1.3	[64] [65] [66] [67] [68]
Danger Theory	Section 2.1.4	[69] [70] [71] [14] [72] [73] [74] [75]
Dendritic Cell Algorithms	Section 2.1.5	[76] [77, 78] [79] [15] [80, 81] [82] [83] [84] [85] [86] [87] [88]
Other Models	Section 2.1.6	[16] [89] [90]
Hybrid Approaches	Section 2.1.6	[91] [92] [93] [94] [95] [96] [97] [98] [99] [100] [101] [102] [103] [104] [105] [106] [107] [108]

Table 2: AIS Algorithms Inspired by Self/Nonself Discrimination Theory

Immune Theory	**AIS Algorithm**	**Key Immune Components**
Self/Nonself Model [109]	Negative Selection Algorithm [6]	T Cell
Pattern Recognition Receptor Model [110]	Conserved Self Pattern Recognition Algorithm [16]	T Cell, APC, PAMP, Signal One, Signal Two
Danger Theory [69]	Dendritic Cell Algorithm	T Cell, APC, Tissue,

Accepted Manuscript

ACCEPTED MANUSCRIPT

	[15] and Danger Theory Application [73-75]	Danger Zone, Signal One, Signal Two

2.1 AIS Models

2.1.1 Negative Selection Algorithms

In biological immune system, T cell precursors move to the thymus from the Bone Marrow and T cell development occurs in the thymus. T cell precursors do not express any of T cell markers such as T Cell Receptor. The stages of T cell development are identified by the expression of specific TCR. Direct cell to cell interaction between Pre-T cells and thymic cells induces Pre-T cells' proliferation and also differentiation. At this point, the alpha-chain of TCR undergoes generic rearrangement. These T cells undergo the processes of Negative Selection to eliminate those T cells that are strongly activated by self MHC plus self peptides in the thymus.

An up to date survey on negative selection algorithms was published in [27]. Though different variations of negative selection algorithms have been frequently proposed, the main characteristics of this method described in [6] still remain, including negative representation of information, distributed generation of the detector set, and one-class classification. Data representation is one of the main aspects of negative selection algorithms; typically, they use either string or real-valued vector representation. In addition, a negative selection algorithm is distinguished by a particular matching rule, which is typically based on a distance or similarity measure. It is important to notice that a matching threshold is also considered to model partial matching for the purpose of approximation and generalization. Our survey found that different variations of negative selection algorithms (NSA) have recently been proposed. These NSA variations are mostly concentrated on developing alternative detector generation schemes to improve the algorithm performance.

Gao et al. [28] introduced a genetic algorithm based negative selection algorithm detector optimization scheme. In this paper, they only focused on optimizing the non-overlapping detectors to obtain the maximal nonself space coverage. To guarantees that for o_j, detector j has the maximal possible radius r_j without any overlapping with all the N self samples, a genetic algorithm is used for the optimization of o_j. The fitness of each detector is calculated by its radius r_j. Those detectors with larger valid radiuses have higher fitness for evolution in the genetic algorithm. A parallel work in [29] presented clonal optimization NSA in which the detectors are optimized by clonal optimization method for anomaly detection. The clonal optimization NSA was tested with simulated bearings fault detection problem.

Shapiro et al. [30] introduced hyper-ellipsoid detectors as an improvement to hyper-spheres detectors in a negative selection algorithm. Shapiro et al. then used an evolutionary algorithm (EA) to optimize the set of ellipsoids. Hyper-ellipsoids retain the benefits of hyper-spheres but are much more flexible, mostly because they can be stretched and reoriented. The experimentation validates the concept that fewer hyper-

ACCEPTED MANUSCRIPT

ellipsoids can cover similar non-self space compared to the traditional hyper-spheres model in a negative selection problem. Another work in [31, 32] introduced hyper-rectangular detectors covering the non-self space, which are created using a niching genetic algorithm and enhanced by a co-evolutionary algorithm.

Luo et al. [33] proposed a novel negative selection algorithm called r[]-NSA with binary representation. In r[]-NSA, each detector, called r[]-detector, has the corresponding array keeping multiple partial matching length (thresholds). Also, Luo et al. [34], proposed a heuristic detector generation method for negative selection algorithm. In this method, a template consisting of $\{0,1,*\}$ is regarded as a candidate detector, where "*" can match with "0" and "1". A template of order *i* represents a template of length *l* with (*l*-*i*) "blank" symbols (*). For example, a candidate detector "11*1*" is a template of order 3 with two "blanks".

Additional research in [35] presented a fast negative selection algorithm by exploiting the ability of a multi-pattern matching algorithm to locate all occurrences of multi-pattern in an input string by only one scan operation. This method converts the self set to a state graph called self graph and efficiently generates the detectors based on the self graph through negative selection. Correspondingly, the detector set is also converted to the detector graph. To determine the anomaly, the partial matching operation is performed between the detector graph and the string to be identified. The time complexity of this method is $O(l)$ compared to $O(N_R \times l)$ of the exhaustive detector generation, with *l* the length of the input string.

Two Evolutionary Negative Selection Algorithms (ENSA) using binary representation were proposed in [36]; they were named *simple* ENSA and *basic* ENSA. In *simple* ENSA, if the detector matches the data, an abnormal change is identified. Otherwise, the initial detector set is evolved to the next generation through mutation, selection and negative selection. Such evolutionary generation loops continue until the abnormal change is detected. The steps in basic ENSA are similar to *simple* ENSA. However, an additional randomly generated detector set is added to next generation detector set in *basic* ENSA. They claimed that the advantage of this change in *basic* ENSA is that it can search in the global space and prevent converging to local optima. Further work in ENSA investigated the ability of the ENSA to detect abnormal change in non-self space [37]. Two mutation operators were used in analyzing the convergence of the ENSA. The first mutation operator (Mutation I) is that only one bit of a detector is selected and flipped with a high probability. The second mutation operator (Mutation II) is that every bit of a detector is possible to be flipped, but the probability is relatively low. The work in [38] discussed the average time complexity of ENSA for two different cases: 1) No gap between the initial detector set (**I**) and the anomaly string samples to be detected (**C**); 2) Gaps exist between **I** and **C**. The time complexity in the first case is $O(l \times \ln(l))$ with a string of length *l*, whereas the time complexity in the second case is $O(l^{g+1})$, *g* is the width of the gap. The ENSA has been applied to hardware/software partitioning problems in embedded systems [39].

ACCEPTED MANUSCRIPT

Ma et al. [40] proposed an antigen feedback mechanism to efficiently generate effective detectors. In addition to the randomly generated detectors, the unmatched antigen is copied into the detector space called feedback detector. This feedback detector goes through the same maturing process as a randomly generated detector to be eliminated if it matches any of the self strings. The matured feedback detector is then used to match further incoming antigens. If it can be activated by the incoming antigens, then it becomes a legitimate detector.

In another work, Chmielewski [41] introduced tree-based structures to represent KDD Cup 1999 data to speed up the performance of V-detector. They used *k-d* tree structure to store self samples to reduce the complexity of searching the nearest self samples. However, they addressed that tree-based structures are not useful for detector generation. [42] used V-detector to detect novelties in Mackey-Glass time series and suggested that the methods for estimation of optimal state-space reconstruction parameters may be used for the estimation of immune-based detection system's parameters.

Stibor et al. [43] proposed the self detector classification method. In this method, self-elements were considered as self detectors with an *a-priori* given self-radius r_s. If an element lies within a self-detector, it is classified as self, otherwise as non-self. The self radius is determined in the training phase by means of a ROC analysis, which is initialized with a small start value (e.g. 0.01) and increased after one training classification run by $r_s = r_s + \Delta i$ until $r_s \geq$ max (e.g. max=1.0). The resulting false alarm rates and detection rates are calculated for every Δi step and used for plotting ROC curves. The self radius r_s that produced the minimum error was selected for the self-detectors. The self detector classification method was compared to both the V-detector and the one class support vector machine (SVM) with the same data sets in [44]. Their experimental results concluded that the self detector classification performed better in general. They also questioned whether real-valued negative selection is an appropriate approach for anomaly detection because it requires positive and negative examples to achieve high classification accuracy.

In additional work, Stibor et al. [45, 46] argued that *holes* in anomaly detection with binary negative selection algorithm are necessary to generalize beyond the training data set. Holes must represent unseen self elements (or generation regions) to ensure that seen and unseen self elements are not recognized by any detector. In [45], they explored the generation capability of the Hamming negative selection when using the r-chunk length *r*. They found that an r-chunk length which does not properly capture the semantic representation of the input data will result in an incorrect generalization and further concluded that a suitable r-chunk length does not exist for input data with element of different length. In [46], they conducted some experiments to investigating how randomly determined permutation masks will influence the occurrence of holes. They observed that holes when applying a randomly determined permutation mask are randomly distributed across the space instead of being concentrated inside or close to self regions because a randomly determined permutation mask shatters the semantical representation of the underlying data. They further pointed out that finding a permutation mask which does not significantly distort the semantical representation of the data may

Accepted Manuscript

be computational intractable and therefore, the use of permutation masks casts doubt on the appropriateness of abstracting diversity in Hamming negative selection. In [47], Stibor investigated the r-contiguous matching probability in a random search approach by using the equivalent k-CNF problem formulation. This work turned out that finding detector is hardest in the phase transition region, depending on the number of self bit strings, the bit string length and matching length. Most recently, Stibor proposed measure distance in binary negative selection by means of probabilities which is modeled with a kernel estimator and advocated that a statically founded method is worthy of being introduced in the area of AIS [48].

Caldas et al. [49] presented a new selection algorithm based on negative selection algorithm and decision theory. A repository database (DB) is used to store quantitative indicators of self performance for an enterprise in the proposed system. Those indicators of self performance are derived from transactional systems and external information. The decision cells are responsible for selecting the appropriate executive decisions from DB and providing the feedback from executive decision making to DB. Each decision cell represents a decision problem and is composed of *n* decision receptors. The proposed algorithm includes two stages: learning and operation. In the learning stage, the decision maker generates the first decision cells based on strategic information stored in DB. These cells make the initial repository of self cells, that is, decision memory, to be stored in DB for future generalizations. In the operation stage, the decision maker requests a decision cell of a specific type from the system. After the most appropriate decision cells have been generated and thereafter presented to a given decision problem, the decision maker may be requested (not always) to decide whether it is self or non-self. Several experiments were carried out to test the proposed algorithm.

Graaff et al. [50] recently presented a genetic artificial immune system (GAIS) in which a life counter function was used to dynamically determine the number of detectors. In GAIS, the status of an artificial lymphocyte (ALC) could be one of four states with different priority: *Immature (no priority)*, *Annihilated (low priority)*, *Mature (medium priority)*, and *Memory (high priority)*. The priority is measured by a life counter (LC) value between 0 and 1. The bit-string receptor of an ALC is randomly initialized then is trained with either the positive selection method or the negative selection method. Each ALC is assigned an affinity-distance threshold, which is the hamming distance of the nearest self pattern to the ALC in negative selection training or the hamming distance of the self pattern furthest from the ALC. When matching a non-self pattern, the number of non-self matches by an ALC will be kept in record using a HitCounter function to determine the ALC's matching ratio. After a specified number of patterns have been classified, the HitRatio of an ALC is calculated by using total HitCounter divided by the number of iterations. The life counter function is introduced in GAIS to determine in which state an ALC is at any given time. The value of the life counter depends on the ALC's HitRatio. Another feature of GAIS is to use Genetic Algorithm (GA) to evolve a dynamic set of ALCs. Each ALC is considered as a chromosome and a set of randomly generated ALCs constitutes the initial populations of the GA. The fitness of an ALC is evaluated differently for different training methods, depending on the average distance between the ALC and the existing set of ALCs, and the ALC's affinity distance threshold.

Accepted Manuscript

ACCEPTED MANUSCRIPT

Parent chromosomes that are randomly selected from an elitist set of chromosomes produces a set of offspring through uniform crossover. Random mutation with probability is applied to randomly selected offspring. The new population selected for next generation includes all individuals in the elitist set and the fittest offspring. The GA stops when the maximum number of generations is reached or the fitness of the ALC population has converged. This work applied the GAIS model to classification problems with 5 different data sets from UCI machine learning repository and compared the proposed model with C4.5.

In [51] a genetic algorithm was used to generate the detector set in a real-valued negative selection algorithm. Each chromosome represents a possible detector set where each gene corresponds to a pointer (index) to a certain *n*-dimension point (detector center) in a sequence of samples with a probability distribution. The detector centers were placed by using highly uniform quasi-random sequences. A decoding function is used to compute the largest possible radius for each detector center. The retained detector set should tolerate self set and have minimum overlaps between the detectors. The volume of the detector set is used to evaluate the fitness of the solution coded in the chromosome. The volume of the detector set and the volume of the self set are calculated by Monte Carlo Integration [52, 53]. The proposed detector generation scheme is suitable for high dimension problems because the error in a Quasi-Monte Carlo integration, which computes the non-self coverage, is related to the number of points used rather than to the problem dimension.

2.1.2 Artificial Immune Network

In 1974, Niels K. Jerne [111] proposed an immune network theory suggesting that immune system is capable of achieving immunological memory by the existence of a mutually reinforcing network of B cells. The B cells not only stimulate each other but also suppress connected cells to regulate the over stimulation of B cells in order to maintain a stable memory. The paratopes of a B cell have the ability to match against idiotopes on other B cell. The binding between idiotopes and partopes has the effect of stimulating the B cells, which forms the immune network called idiotypic networks.

Based on Farmer et al.'s immune network model [7], the artificial immune network algorithm proposed by Ishida [8] can be considered as the earliest work in the field of AIS. These earlier works were further improved by Hunt et al. [112]. Their proposed system was composed of a bone marrow object, a network of B cell objects and an antigen population. The B cell object population is randomly initialized by the bone marrow object. When the antigen population is loaded to the system, they are randomly picked up and inserted to a randomly chosen point in the B cel network. If the B cell can bind to the antigen population, may new B cell objects will be cloned and the clones with higher affinity to the cells already in the network will be added to the existing network of the B cells. The work in [113] refined the initial model. The new implementation in Jave with a relational database is called *Jisys*. In *Jisys*, a B cell population is divided into two sub-populations: the initial population and the clones population. The initial B cell population is generated from a subset of raw training data. The antigens are selected

Accepted Manuscript

ACCEPTED MANUSCRIPT

randomly from the remaining training data and presented to the area of the B-cell network. *Jisys* also adopted the techniques developed by CBR (case based reasoning) community and used various methods borrowed from Genetic Algorithm and other techniques to clone the B cells (network nodes).

Such artificial immune networks were later re-defined and re-implemented by Timmis et al. [9] and further enhanced in [114]. Earlier AINE related work include enhanced AINE, re-implementation of AINE, Fuzzy AINE and dynamically weighted AINE [115-123]. AINE incorporated some basic ideas from the clonal selection theory. The B cells in AINE undergo cloning, mutation and selection when they are simulated in the network. aiNet is a learning algorithm and performs clustering of input data in such a way that the MSE (mean square error) is iteratively reduced [124]. Although it is generally considered as one of the AINE family and is still considered in that category in this review, aiNet takes its inspiration from clonal selection theory. For example, an activated (recognized) input pattern (antigen) in aiNet goes through proliferation, mutation and selection. Subsequently, opt-aiNet was developed for solving multi-modal function optimization problems [125]. It introduced several interesting features: 1) it can dynamically search an optimum population size based on the network suppression threshold and a well-defined stopping criterion; 2) it has capability of combining exploitation with exploration of the fitness landscape; 3) it employs both local and global search methods for new and better solutions; 4) it locates and maintains stable local optimal solutions.

Pacheco et al. [7] presented an Abstract Immune System Algorithm [54] based on Farmer et al.'s model. Four facts are considered for the dynamics of this model: 1) the stimulation between the paratope of an antibody and the epitope of another antibody; 2) the suppression of the antibody when its epitope is recognized by the paratope of another antibody; 3) the stimulation between the antigen and antibody; 4) tendency of cells to die in the absence of any interaction. When the reaction loops start, the concentrations of the various antibody types are updated using the finite different method. A given antibody type is stimulated or eliminated by referring to *recruitment threshold* or *death threshold*, respectively. This paper provided two examples used to test the algorithm: a classical maximization problem and the Iterated Prisoner's Dilemma problem.

The work by Schmidtchen and Behn [55] investigated a minimalistic model of idiotypic network of B-lymphocytes where idiotypes are represented by bitstrings encoding the nodes of a network. A given B-cell has exactly one specific type (the idiotype) of antibody. The entirety of the B-lymphocytes system forms a functional network consisting of all idiotypes an organism is able to generate and the links connecting complementary idiotypes allowing a few mismatches. The idiotypic network is modeled by an undirected base graph $G=(\nu,\varepsilon)$. Each idiotype $\nu\in\nu$ in the network is characterized by a bitstring of length *d*: $b_d b_{d-1}...b_1$, with $b_i\in\{0,1\}$ for all $i\in\{1,2,...,d\}$ [56]. This work performed simulations on the base graph $G_{12}^{(2)}$ for (t_l, t_u) = (1, 10) for different values of influx *I* starting with an empty base graph. The base graph contains 4096 nodes each of which has 79 links to other nodes. The simulations showed that after a transient period a steady state is achieved. The random evolution leads to a network with highly organized architecture. The nodes can be classified into different

Accepted Manuscript

ACCEPTED MANUSCRIPT

groups with clearly distinct statistical properties. The major contribution of this work is explaining these very complex network structures emerging during the random evolution through a detailed analytical understanding of the building principles. The building principles allow us to calculate instance size and connectivity of the idiotype groups in perfect agreement with the empirical findings reported in [56].

In [57], omni-aiNet was developed to solve single and multi-objective optimization problems, either with single and multi-global solutions. omni-aiNet united the concepts of omni-optimization with distinctive procedures associated with immune-inspired concepts and thus showed several advantages: 1) automatically adapting the exploration of the search space according to the intrinsic demand of the optimization problem; 2) adjusting its size during the execution of the algorithm, according to a predefined suppression threshold; 3) controlling the spread of solutions in the objective space with a new grid mechanism.

By exploiting the multipopulation property of aiNet, a Multi-Objective Multi-population Artificial Immune Network (MOM-aiNet) for biclustering was proposed [58]. A distinction of MOM-AiNet from other multi-objective optimization algorithms is that MOM-aiNet returns several sets of non-dominated solutions as opposed to only a single set of non-dominated solutions. The concept of dominance is generally used to compare the quality of two solutions for a given problem, and so it is used to measure the solution set returned by MOM-aiNet. Biclustering can produce arbitrarily positioned and possibly overlapping biclusters, which is the case of MOM-aiNet. Each set of non-dominated solutions in MOM-aiNet potentially corresponds to biclusters extracting distinct correlations of rows and columns of the data matrix. By randomly choosing one row and one column of the dataset, MOM-aiNet first generates *n* subpopulations of one bicluster. In the algorithm, for each subpopulation, *n-clones* clones are generated subject to a mutation process. The mutation consists of one of three possible actions chosen randomly with the same probability: insert a row, insert a column, and remove a row or column. If the number of non-dominated elements exceeds *n-clones*, a crowding distance-based suppression is performed in order to maintain a small and locally diverse subpopulation. The MOM-aiNet al.gorithm was applied to both Yeast problem and the Movielens dataset and was compared with FLOC, CC and BIC-aiNet al.gorithms in this work. In spite of its enhanced performance as compared to the other algorithms, the results showed that MOM-aiNet can best control the bicluster quality and return a broader set of non-dominated solutions.

Another variant of opt-aiNet called opt-aiNet-AA-Clust was proposed and implemented in [59]. A new representation for proteins was proposed in this work, in order to maximize the predictive accuracy of a hierarchical classification algorithm applied to protein function prediction. Earlier work [60, 61] divided the amino acids into three functional clusters: hydrophobic (amino acids C,V,L,I,M,F,W), neutral (amino acids G,A,S,T,P,H,Y), and polar (amino acids R,K,E,D,Q,N). This work borrowed this idea to substitute the amino acids in the sequence for the cluster to which that amino acid belongs. A good example in this paper is that assuming H=hydrophobic, N=neutral and P=polar, the protein sequence CVGRK would be converted to HHNRR. This work

ACCEPTED MANUSCRIPT

defined three local descriptors: composition (C), transition (T), and distribution (D). C is the proportion of amino acids with a particular property. T is the frequency with which amino acids with one property are followed by amino acids with a different property. D measures the chain length with which the first, 25%, 50%, 75% and 100% occurrences of the particular property are located. A detailed example was provided in this paper to demonstrate how to calculate these three local descriptors. This work then proposed an Artificial Immune System (AIS) for amino acid clustering. Although this work only dealt with structures where each class has exactly one parent, the experimental results showed that a significant increase in predictive accuracy was at the third level of the class hierarchy. Further work may be needed to investigate this contradictive result. Another variation of opt-aiNet [62] was developed for the capacitor placement problem for radial distribution networks. This variation uses an integer value vector to represent the network cell for possible solution. It has no control over the initialization process and applies a fixed mutation rate.

In another work Stibor et al. [63] investigated the compression quality of aiNet. Based on the Parzen window estimation and Kullback-Leibler divergence, they presented a similarity measure between the input data set and the aiNet output data set. A Parzen window estimator is used to estimate the probability densities over the input data set and output data set. This paper provided the source code to generate data sets from different probability distributions written on open source program *R*. The experiments with four generated data sets revealed that aiNet performs better on a uniformly distributed data set, whereas it produces poor results on non-uniformly distributed data set.

2.1.3 Clonal Selection Algorithm

Clonal Selection Theory states that a clonal expansion of the original lymphocyte occurs when the original lymphocyte is activated by binding to the antigen; however, any clone of the activated lymphocyte with antigen receptors specific to molecules of the organism's own body (self-reactive receptors) is eliminated during the development of the lymphocyte. During the clonal expansion of B cells, the average affinity increases for the antigen that triggered the clonal expansion through a process of affinity maturation. Therefore, the memory B cells are developed to make a more effective immune response to antigens that had been encountered. Affinity maturation is caused by a somatic hypermutation and a selection mechanism. Somatic hypermutation results in the diversity of antibodies by introducing random changes to the genes that encode for them. The selection mechanism guarantees that only those clones (antibodies) with higher affinity for the encountered antigen will survive. On the basis of Clonal Selection Theory, Clonal selection algorithm was initially introduced in [11] and formally described in [12]. The general algorithm was named CLONALG.

Work by Ciccazzo et al. [64] introduced a new clonal selection algorithm called the elitist Immune Programming (EIP). EIP was an extension of Immune Programming (IP) and the pseudo-code of EIP was provided in this paper. Firstly, the concept of *elitism* borrowed from other immune inspired algorithm is introduced to EIP; that is, at each generation *g*, the best solution found so far cannot be erased from the population. In addition, EIP uses

Accepted Manuscript

ACCEPTED MANUSCRIPT

a new class of hypermutation operators and a network-based coding. A hypermutation operator acts on one component, link or node at a time. All the operators take or return only consistent circuits. This work introduced ten ad-hoc network-based hypermutation operators, including add-series, add-parallel, add-random-component, expand-node, delete-component, mutate-component-value, copy-component-value, mutate-component-kind, link-modify, and shrink. This work applied the EIP algorithm to the synthesis of topology and sizing of analog electrical circuits. The quality of the circuit was assessed by the distance between the curve described by a circuit and the one described by a hypothetical ideal circuit. The experiments showed that the circuits obtained by EIP were better than the one found by Genetic Programming.

Halavati et al. [65] added the idea of symbiosis to CLONALG. As a variation of CLONALG, this algorithm uses partially specified antibodies that may not have all required data to be evaluated as a solution. This algorithm is initialized with a set of partially specified antibodies, each having just one specified property. Then, the algorithm randomly picks an antibody to add to an assembly. By repeatedly doing so, the algorithm shall build an assembly with all required properties. If the algorithm fails to complete such assembly with existing antibodies, it will create some antibodies with random values for all missing positions of the created assembly and add them to the population. The process of cloning, mutation and selection in this algorithm is extremely similar to those in CLONALG. As stated in this paper, the inspiration of using partially specified antibodies comes from the assumption that a problem can be broken into several sub-problems and thus good solutions of these sub-problems may compose a general good solution for the main problem. If such assumption becomes true, this algorithm may find a solution faster than CLONALG. By applying them to multimodal function optimization and combinatorial optimization, this work showed that the proposed algorithm can solve problems that CLONALG failed to solve.

The work in [66] presented a variation of CLONALG for software mutation testing. The variation allowed several memory individuals to contribute to the recognition of an antigen, rather than following the concept of a memory individual per antigen in CLONALG. Each antibody represents a single test in this application. The population of antibodies is initialized with *s* tests, either by randomly generated tests or pre-specified ones. The algorithm iteratively searches for those antibodies that will kill at least one mutant program that has not already been killed by an existing memory test. The mutation score (MS) is used to evaluate the affinity (or fitness) of an antibody. Those antibodies with high affinity are added to the memory set to be returned to the tester at the end of the process. The process of antibody evolution (clone selection) in this variation is same as that in CLONALG. The effectiveness of this variation of CLONALG was compared against an elitist genetic algorithm and the results showed that the Immune Inspired Approach generates higher mutation scoring test sets with less computational expense.

Inspired by the clonal selection principle, work in [67] developed an immune algorithm for the protein structure prediction problem on lattice models. Antigen (Ag) and B cells in the proposed immune algorithm represents a sequence of hydrophobic-pattern of the

Accepted Manuscript

ACCEPTED MANUSCRIPT

given protein $s \in \{H, P\}^{\ell}$ and a sequence of directions $r \in \{F, L, R\}^{\ell-1}$, respectively. H, P denotes two types of beads in the standard Dill's lattice model: bead-Hydrophobic/non-polar or bead-hydrophilic/Polar, respectively. F, L, R denotes Forward, Left, and Right, respectively. ℓ is the number of amino acid in the protein sequence. Different from the original Clonal Selection Algorithm, this work proposed two special mutation operators (inversely proportional hypermutation and hypermacromutation) and one aging mechanism. Inversely proportional hypermutation is similar to the mutation operator in the conventional Clonal Selection Algorithm. It makes mutations inversely proportional to the fitness value. The hypermacromutation operator randomly determines the number of mutations, which doesn't use functions depending on constant parameters. The aging operator is designed to avoid getting trapped in local minimum by eliminating old B cells from the population based on the maximum number of generations allowed for generated B cells to remain in the population. This work also discussed the characteristic dynamics of the proposed immune algorithm and demonstrated the competitive performance of the algorithm by testing with well-known protein structure prediction lattice models, the HP model in two-dimensional and three-dimensional square lattices, and the functional model protein.

Wilson et al. [68] proposed Trend Evaluation Algorithm (TEA) to evaluate price time series data. TEA is very similar to CLONALG with some differences that are summarized in this paper. TEA not only finds the best fitting candidates (long term memory pool) but also maintains short term memory pool by proliferating all bound trackers. Apoptosis and mutation in the TEA occurs across all population members. A simple antigen *A* containing 20 fictitious price movements and 8 trends (*T1* to *T8*) is constructed to test the ability of the TEA to identify price trends. Antigen *A* is further splitted into two subsets *A1* an *A2*. A1 contains three simple trends T1, T2, and T3 and the other more complex trends are involved in A2. 4 experiments were defined in this work to examine the algorithm's ability to identify the price trends and to investigate the influence of the long term memory pool.

2.1.4 Danger Theory Inspired Algorithms

The Danger Theory has become popular among immunologists for the last decade. Its chief advocator, Polly Matzinger, proposed this theory in 2002 in the journal Science [69]. She points out that the "foreignness" of a pathogen is not the important feature that triggers a response, and "selfness" is no guarantee of tolerance. The central idea in the Danger Theory is that antigen presenting cells (APCs) are activated by danger/alarm signals from injured cells, such as those exposed to pathogens, toxins, mechanical damage, and so forth. However, danger/alarm signals should not be sent by healthy cells or by cells undergoing normal physiological deaths. Alarm signals can be constitutive or inducible, intracellular or secreted, or even a part of the extracellular matrix. Cells that die necrotically release their contents. Any intracellular product could potentially be a danger signal when released. Inducible alarm signals could include any substance made, or modified, by distressed or injured cells.

Accepted Manuscript

ACCEPTED MANUSCRIPT

According to the Danger Theory, a cell that dies unnaturally sends outs the danger/alarm signal. The danger signal establishes a danger zone around itself. On the other hand, the antigens near the cell that emits the danger signal are captured by APCs such as macrophages, and then travel to the local lymph node and present the antigens to lymphocytes. The antibodies secreted by B cells match the antigens, but only those that match the antigens in the danger zone will be activated or stimulated and will undergo the clonal expansion process. Those that do not match or are not in the danger zone will not become stimulated.

Bretscher and Cohn extended the Two-Signal model that takes into account the danger model in another way [70]. The lymphocytes need two signals to become activated: antigen recognition (signal one) and co-stimulation (signal two). Co-stimulation is a signal that means “this antigen really is dangerous”. Polly Matzinger [71] further applied the laws of lymphotics to the danger theory:

- Law 1: Two signals are needed to activate the lymphocyte. The lymphocyte will die if it receives signal one without the costimulation of signal two. In the absence of signal one, signal two will be ignored.
- Law 2: Signal one can come from any cell. However, signal two comes from APCs, however, the signal two for B cell activation comes from T helper cells.
- Law 3: Activated (effector) cells do not need signal two, which revert to resting state after a short time. Immature cells are unable to accept signal two from any source.

Although a number of advantages are claimed by the Danger Theory, it does have several limitations. Matzinger admits that the exact nature of the danger signal is unclear. The danger theory has yet to clearly answer this question: how to distinguish danger from non-danger? Also, there are sometimes dangers (cuts, transplants) that should be responded to. The autoimmune diseases have not been fully reconciled with the Danger Theory either.

The first paper that proposed an application of the Danger Theory was published in 2002 by Aickelin et al. [14]. This paper pointed out some analogies to artificial immune systems in the Danger Theory, which are highlighted in the following points:

- An antigen presenting cell is required to present an appropriate danger signal.
- The “Danger” signal may have nothing to do with danger.
- The appropriate danger signal can be positive (presence of signal) or negative (absence of signal).
- A measure of proximity may be used to mimic the danger zone.
- An immune response should not lead to further danger signals.

This paper then proposed some conceptual ideas on how the Danger Theory can help overcome several problems when the current artificial systems apply to the application area of anomaly detection. According to the Danger Theory, danger signals should be the ones that trigger an immune response. The suitable signals could include lower or higher

Accepted Manuscript

ACCEPTED MANUSCRIPT

memory usage, inappropriate disk activity, unexpected frequency of file changes and so forth. Once the danger signal has been produced, the immune system can then react to those antigens with the danger zone. The danger zone can be substituted with more appropriate causality measures such as similar execution start times, concurrent runtimes or access of the same resources. The antibodies or detectors that match those antigens (first signal) within a radius defined by a measure (signal two) will undergo proliferation to develop memory cells. Once the dangerous components are identified, they are sent to a special part of the system for further confirmation. Similar application of the Danger Theory to intrusion detection can be also found in [72].

The work in [14] also outlined another illustrative scenario that applies the Danger Theory to data mining problems: a user is browsing a set of documents. Each document has a set of features (keywords, title, author etc). An artificial immune system is implemented and the antibodies in the system are specific for recognizing those features in the documents. Every document browsed by the user will be presented to the antibodies (Signal one). When a user either explicitly or implicitly indicates interest in the current document (danger zone), a "danger" signal is raised (signal two), then those antibodies matching any antigen, i.e., the feature in current "Interesting" document), are stimulated and become effectors. Uninteresting document features will tolerate the autoreactive antibodies in the absence of signal two. The artificial immune system finally learns to become a good filter when searching for other interesting documents.

Prieto et al. [73] applied Danger Theory to a goalkeeper strategy in robot soccer. An algorithm called DTAL (Danger Theory Algorithm) that takes into account danger signals, lymphocytes and the danger zone was developed in this work, including a dynamic danger zone version and a fixed danger zone version. The developed algorithm was used to implement a goalkeeper strategy in robot soccer, particularly, in the middle league SIMUROSOT from FIRA. Specifically, when the ball is on the home side (tissue), the alarm signal (signal one) is triggered; when an opponent takes the ball (antigen) near the penalty area (danger zone), signal two is triggered; when both danger signals are received, a lymphocyte is activated to clear the ball. The developed strategy performed well with effectiveness above 90%.

Iqbal et al. [74] introduced a novel intelligent data processing approach inspired by Danger Theory. This work identified the presence of DASTONs in system call data by correlating system call sequences of normal and exploited processes. DASTONs represent the data chunks or points present in a data heap that actively participate in data processing to retrieve specific information from the data. The result is useful because taking care of DASTONs will make the system more efficient by reducing the amount of data to be processed.

Another work in [75] highlighted some initial ideas on how the Danger Theory could be used to further improve the performance of an e-mail classifier system. For example, in a web mining system, different types of media may cause different types of signals to be released, whereas in an e-mail system, an out of the ordinary e-mail may release an "interesting" signal of one class. The strong relevance of these features can be found

Accepted Manuscript

ACCEPTED MANUSCRIPT

through Danger Theory. However, Secker et al. [75] stated that some highly related research questions still remain unanswered.

2.1.5 Dendritic Cell Algorithms

The Dendritic Cell Algorithm (DCA) is inspired by innate immunity, more precisely, the function of dendritic cells. Dendritic cells, whose primary role is as antigen presenting cells, were originally identified by Steinman and his colleagues [76]. Dendritic cells comprise a system of leukocytes widely distributed in all tissues. They possess a heterogeneous hemopoietic lineage and so perform a differential morphology, phenotype and function in different tissues. Dendritic cells are derived from bone marrow progenitors and circulate in the blood as immature precursors prior to migration into peripheral tissues. Within different tissues, dendritic cells differentiate and undergo further maturation when appropriately stimulated; then they migrate to secondary lymphoid tissues where they present Ag to T cells and induce an immune response.

The immature dendritic cells (proliferating progenitor cells and non proliferating precursors) reside at body surfaces and interstitial spaces. In most tissues, dendritic cells are present in a so-called immature state and are unable to stimulate T cells. They have abundant major histocompatibility (MHC) II products within intracellular compartments and respond rapidly to inflammatory cytokines and microbial pathogens to produce mature T cell stimulatory. Once the immature dendritic cells have acquired and processed the foreign pathogens, they migrate to the thymus and the spleen, undergo maturation and stimulate an immune response.

Regarding their state of maturation, dendritic cells can perform different functions. As described in [77, 78], modulation between these states is facilitated by the detection of signals within the tissue – namely danger signals, PAMPs (pathogenic associated molecular patterns), apoptotic signals (safe signals) and inflammatory cytokines. The characteristics of these four types of signals are summarized as follows:

- PAMPs are pre-defined bacterial signatures, causing the maturation of immature dendritic cells to mature dendritic cells through expression of “mature cytokines”.
- Danger signals are released as a result of damage to tissue cells, also increasing mature dendritic cell cytokines, and have lower potency than PAMPs.
- Safe signals are released as a result of regulated cell death, cause an increase in semi-mature dendritic cells cytokines, and reduce the output of mature dendritic cell cytokines.
- Inflammatory cytokines are derived from general tissue distress and amplify the effects of the other three signals but are not sufficient to cause any effect on immature dendritic cells when used in isolation.

The maturation state of a dendritic cell influences the T cell response and it is determined by the relative concentrations of these four types of signals. Based on the combinations of the received signals, two terminal differentiation states, namely, mature or semi-mature, are generated during the maturation of dendritic cells. The mature dendritic cells exhibit

Accepted Manuscript

ACCEPTED MANUSCRIPT

the following behavior: collection of antigen ceases; expression of co-stimulatory molecules and chemical messengers (cytokines); migration from the tissue to a lymphatic organ; and presenting antigen to T lymphocytes [79]. Mature dendritic cells have an activating effect while semi-mature dendritic cells have a suppressive effect.

The first dendritic cell algorithm was conceptualized and developed by Greensmith et al. [15]. It is characterized by combining multiple signals to assess the current context of the environment and asynchronously sampling another data stream (antigen). The input signals have to be pre-classified, including PAMPs (abnormal), safe signals (normal), danger signals (possible changes), inflammatory cytokines (signals that amplify the effects of the other signals). However, inflammatory cytokines were not considered in this paper. A fuzzy threshold, derived in proportion to the concentration of costimulatory molecules, is used for a dendritic cell to stop collecting antigen and migrate from the sampling pool to a virtual lymph node. The dendritic cell algorithm processes the input signals with the pre-defined weights to produce three output signals (costimulation signal, semi-mature signal and mature signal). If the cumulative mature signal is greater than the cumulative semi-mature signal value, then the cell differentiates towards a mature state and is assigned a "context value" of 1, and opposite. The algorithm then calculates the proportion of the mature context presentation of that particular antigen, relative to the total antigens, termed "MCAV (mature context antigen value)" of that antigen. The antigens with a MCAC which exceed a predefined threshold are classified as anomalous.

A formal description of the dendritic cell algorithm is given in [80]. The dendritic cell algorithm is implemented as a libtissue tissue server and has three stages: initialization, update and aggregation. Initialization involves setting various parameters. The update stage can be decomposed into tissue update and cell cycle. The tissue update and cell cycle form the libtissue tissue server. Signal data is fed from the data-source to the tissue server through the tissue client. The tissue update occurs on an event-driven basis. When the new data appears in the system, it updates the values for signals and for the antigen to provide the input signals for the population of the dendritic cells. The cell cycle is a discrete process occurring at a user defined rate. The cell cycle and tissue update continues until a stopping criterion is reached, usually when all of the antigen data is processed. The last stage is aggregation, where all collected antigens are subsequently analyzed and the MCAV per antigen is derived. The graph and pseudocode are provided to explain the data structure and three stages in the dendritic cell algorithm, respectively. The semantics of the different category of input signals are summarized as follows:

- PAMP: 1) a signature of abnormal behavior; 2) a high degree of confidence of abnormality associated with an increase in this signal strength.
- Danger signal: 1) the measure of an attribute which significantly increases in response to abnormal behavior; 2) a moderate degree of confidence abnormality with an increased level of this signal, though at a low signal strength it can represent normal behavior.
- Safe signal: 1) a confident indicator of normal behavior in a predictable manner or a measure of steady-behavior; 2) the measure of an attribute which increases signal concentration due to the lack of change in strength.

ACCEPTED MANUSCRIPT

- Inflammatory signal: 1) a signal which cannot cause maturation of a dendritic cell when the other signals are not present; 2) a general signal of system distress.

Gu et al. [81] applied the dendritic cell algorithm to the KDD 99 data set and added two additional functions to the system for the purpose of optimization: antigen multiplier and moving time windows. To overcome the problem of "antigen deficiency", the antigen multiplier makes several copies of each individual antigen which can be fed to multiple dendritic cells. With the moving time windows, the new signals are calculated in each iteration. The results suggest that the antigen multiplier and moving time windows have the same effect on the dendritic cell algorithm for the KDD 99 data set.

Oates et al. [82] proposed a solution to a robotic classification problem based on the dendritic cell algorithm (DCA). The robotic dendritic cell algorithm is implemented as a stand-alone behavioral module for compatibility with subsumption architecture. It extends the Aria library's 'wander' architecture with two additional modules: image processing and DCA executing. The DCA module outputs MCAV coefficients, approximately once per second. Three signals are used as inputs to the DCA: PAMP, safe and danger. The PAMP is originated from the image processing module. The LRF is the source of the safe signal. The sonar array which has a 3600 FOV is considered as the danger signal. For the implementation in this paper, the antigen is an integer number which uniquely identifies a segment of the test pen indicating the positions and orientations of the robot.

The original dendritic cell algorithm is highly stochastic. In contrast, a Deterministic Dendritic Cell Algorithm (dDCA) was developed in [83]. In dDCA, signals of at least two categories and antigens are required. A uniform distribution of lifespan values is used across the population. Each dendritic cell in the population is exposed to identical input signals and processes these signals in an identical manner. One further modification is that the random sampling and storage in the previous implementation of the DCA is replaced by a simple array, which is used to store the value of the antigen and the number of times a dendritic cell has collected antigens of this type. The dDCA only contains three parameters: the number of dendritic cells, the weighting schema for the signal processing, and the output context value of an individual dendritic cell (only one factor *k*). The signal processing equation is also modified in dDCA. In dDCA, K_α is used as a measure of the proportion of antigens presented by a fully mature cell to replace MCAV in the original DCA. K_α is used to generate real valued anomaly scores encapsulating the magnitude of the difference between normal and abnormal processes. This work also examined the effects of the use of time windows, the variation of the number of cells and discussed the influence of both parameters in the algorithm. [84] is another recent work related to the DCA, which investigated the suitability of both classical DCA (cDCA) and deterministic DCA (dDCA), for malware detection at run-time.

The work in [85] illustrated how closely the dendritic cell algorithm matches the structure and functional requirements of sensor networks and further presented a variation of DCA called ubiquitous DCA (UDCA) to detect "Interest Cache Poisoning Attacks" on sensor networks. In [85], UDCA is characterized as follows:

ACCEPTED MANUSCRIPT

- A dendritic cell in UDCA collect signals from multiple data sources by continuously accumulating new output cytokines at each dendritic cell maturing cycle.
- UDCA maps the context information with antigens in a temporal manner: antigens (interests) are gathered when signals that deliver context information are generated.
- The context status of a given antigen in UCDA is judged by multiple signals and the collective decisions of multiple dendritic cells.
- UDCA detects an attack by examining how much a given node is misbehaving via generated signals.

In [86] they applied the dendritic cell algorithm to the detection of outgoing port scans using TCP SYN packets. The TCP SYN scan itself is used to determine which ports are open and which services are running on specified hosts. It is an ideal model of an intrusion and leaves no trace in the normal system logs. In comparison to their earlier work, this work uses the same antigen representation but the signals chosen differ from those in the earlier work. SYN scan detection used seven signals. Two PAMPs signals are taken from data sources which indicate a specific scan. PAMP-1 is the number of ICMP ‘destination unreachable’ error messages received per second. PAMP-2 is the number of TCP reset packets sent and received per second. Two danger signals and two safe signals are derived from attributes which represent changes in behavior. The first danger signal (DS-1) is derived from the number of network packets sent per second, whereas DS-2 is the ratio of TCP packets to all other packets processed by the network card of the scanning machine. The values for safe signals are inversely proportional to the changes in magnitude: the smaller the changes, the higher the values of safe signals. The first safe signal (SS-1) encapsulates the change rate to send network packets. SS-2 is the average network packet size, which drops to a size of 40 bytes during SYN scans. One inflammatory signal is simplified as a binary signal. If a remote root log-in is detected, then this signal is set to 1. Otherwise, it is set to 0. Both passive normal and active normal datasets were used in the experiments. The passive normal dataset emulates a ‘night time’ scan; this scan should make it relatively easy to detect anomalous behavior in this data set since the machine is not being actively used at night. The active normal dataset includes simultaneous web-traffic and scanning processes. Results showed that the DCA performed well with TCP SYN scan detection except that some false positives were encountered when simultaneously scanning and using other network services. This work has been further extended in [87], which pointed out that dendritic cells perform information fusion which directs immune responses.

Another application of the dendritic cell algorithm was presented in [88]. This work proposed and implemented a dendritic cell based distributed misbehavior detection system named BeeAIS-DC for a bioinspired Mobile Ad Hoc Network (MANET) routing protocol, BeeAdHoc. The authors stated that this detection system not only enables BeeAIS-DC to dynamically adapt its detector set to cater for a changing self due to the mobility of nodes, but also that it is robust enough to provide significantly smaller false positives as compared to self/non-self based AIS.

Accepted Manuscript

ACCEPTED MANUSCRIPT

2.1.6 Other newly developed models

Conserved Self Pattern Recognition Algorithm (CSPRA)

The Conserved Self Pattern Recognition Algorithm (CSPRA) [16] is one of the latest developed AIS models inspired from Pattern Recognition Receptors (PRRs) Model [110, 126]. According to PRRs Model, the self/nonself discrimination requests co-stimulation from APCs but APCs do not co-stimulate unless activated via encoded PRRs that recognize conserved pathogen-associated molecular patterns (PAMPs) on bacteria. Obviously, the PRRs model added additional layer of PAMPs to the Self-nonself model but kept the features of Self-nonself model. CSPRA naturally involves negative selection since it is inspired from the PRRs model. However, the anomaly detection in CSPRA is done by combining the results from APCs self pattern recognition and T cell negative selection. APCs self pattern recognition is not conducted unless the anomaly called suspicious antigen cannot be confidently detected by T cell negative selection. The APC detector represents for the conserved self pattern that are extracted from the collected "Self" data. The generation of APC detector includes two major steps:

1) Based on the relationship between the antigen objects and the dimensions of their feature space, to define the *conserved self pattern* that can be pre-defined from the empirical data based on the scientists' lab results or can be derived from the results by calculating the Pearson coefficient *r* between the values in the column of each attribute and their corresponding class labels.
2) Within the conserved self pattern consisting of the features located in *loc1*, *loc2* , *…* , generate APC detector *R*={<*loc1*, *min*, *max*, *mean*>, <*loc2*, *min*, *max*, *mean*>, *…*} by calculating maximum, minimum, and mean of all of the values in the features (or descriptors) of *loc1*, *loc2*, *…* , respectively.

The experiments results from the experiments with this algorithm have suggested that the CSPRA shows promise in assisting in reducing the number of false positive errors without increase the complexity as compared to the classical Negative Selection Algorithm (NSA).

Toll-like Receptor (TLR) Algorithm

TLR algorithm [89, 127] was based on two populations of interacting cells, namely DCs and T-cells. The DCs are created as immature detectors for collecting antigen from an antigen store and process signals for a finite specified period of time. The DC is termed mature if it receives a signal during antigen collection. Otherwise, it is termed semi-mature. Once the DC's lifespan is complete, the DC is transferred to a "lymph node" in which the antigen presented by the DC is matched against a population of T-cells. If a T-cell matches antigen presented by a mature DC, the state of the T-cell is set as "activated". If the T-cell matches the antigen presented by semimature DCs, it is removed from the population. A session is classified as "anomalous" if a population of activated T-cells (one or more) is generated.

Accepted Manuscript

ACCEPTED MANUSCRIPT

The signals used in the TLR algorithm are more analogous to PAMP signals and simplified as binary signals: “signal present” or “signal not present”. An infectious signal list is initially generated to cover all possible signal values. Two things are done in training phase by means of negative selection: 1) It deletes the values of signals seen during training from the infectious signal list, resulting in a list of “nonself” signal values; 2) It generates a population of matured T-cells. The initial T-cell population is matched against normal antigen data and any T-cell matching a normal antigen is deleted from the population. During the testing phase, when the TLR algorithm detects the new coming data, DCs mature upon the activation by any signal from the list of “nonself” signal values. The detailed steps in the TLR algorithm can be found in [89]. The TLR algorithm achieves false positives rates of 0.15 and true positive rates of 0.75 when it was evaluated on a system call anomaly detection problem.

Complex Artificial Immune System

In [90] they proposed a model called CAIS (Complex artificial immune system). CAIS consisted of five layers: encountered layer (Ag layer), preprocessing layer (APC layer), MHC layer, competitive layer (Th cell layer) and stimulation -inhibition layer (B cells layer). Antigen and antibody are considered as input and output respectively. When an antigen is presented to the system, it can be recognized through two different routes. One is B cell direct recognition and the other one is through the APC layer processes. The input antigen is taken by the APC layer; the complex form of the input antigen is translated to MHC layer as the output of the APC layer for further processing. In the MHC layer the information coming from the APC layer is transformed and translated to the Th layer. In Th cell layer, Th cells receive different stimuli from the MHC layer and compose a neighborhood set that consists of some Th cells which have better response to the current input pattern. B cells become activated when receiving co-stimulation by input antigen pattern and stimuli from Th cells located in neighborhood set. An antibody is regarded as the difference between an input pattern and the weights associated with B cells. According to the antibody, Ts cells modulate the weights associated with immune cells located in neighborhood set. Compared with the traditional binary immune systems, the CAIS has a characteristic of invariant feature to recognize transformation, such as translation, scale or rotation of patterns. CAIS was tested on a pattern recognition problem, particularly, on recognizing handwritten digits and it show good immune memory acquisition and noise tolerance abilities.

Hybrid Approaches

By replacing the mutation and cloning operators with a probabilistic model, a Bayesian Artificial Immune System (BAIS) has been developed for efficiently solving hard optimization problems such as the effective handling of building blocks [92] and multiobjective optimization [91]. BAIS replaces the traditional mutation and cloning operators with a probabilistic model capable of properly capturing the most relevant interactions among the variables of the problem. The proposed algorithm adopted artificial immune system to implement the population-based search strategy and a

Accepted Manuscript

ACCEPTED MANUSCRIPT

Bayesian network to implement the probabilistic model. After the population is randomly initialized, BAIS starts the loop that is controlled by a stopping condition. BAIS executes these steps for each loop: 1) evaluate the population to select the best solutions (antibodies) using any selection mechanism; 2) build a Bayesian network that better fits the selected solutions; 3) sample a number of new antibodies based on the generated Bayesian network; 4) eliminate the antibodies with lower fitness and similar antibodies; 5) insert a small percentage of randomly generated antibodies to maintain diversity. [92] showed the ability of BAIS to handle non-overlapping and overlapping building blocks in the single-objective Trap-5 optimization problem. BAIS was also applied to perform feature selection using wrapper approach in [92, 93]. The work in [91] extended BAIS for solving multi-objective Knapsack optimization problems. The corresponding proposal is called Multi-objective Bayesian Artificial Immune System (MOBAIS). The article [94] applied MOBAIS to feature selection in classification problems. Conceptually, MOBAIS is capable of identifying and preserving building blocks effectively while it is able to perform a multimodal search and find diverse high-quality local optimal quickly. The experiments in [94] demonstrated that MOBAIS found parsimonious subsets of features and thus enhanced the accuracy of the classifiers. In [95], MOBAIS were applied to more challenging problems such as multi-objective Knapsack problem and Deb's Test Functions. Furthermore, [95] enhanced the Bayesian network learning by avoiding the synthesis of the Bayesian network at each iteration and only updating two parameters of the Bayesian network, e.g., the conditional and marginal probabilities), at each iteration.

In [96], an unsupervised structure damage classification algorithm based on the data clustering technique and the artificial immune pattern recognition is presented. This technique uses the Data Clustering to cluster training data to a specified number of clusters and generate the initial memory cell set. By integrating with the Artificial Immune Pattern Recognition (AIPR) algorithms, this method provides a mechanism for the evolution of memory cells.

In [97], a combination of an artificial immune and support vector machines for fault diagnosis of induction motors is proposed. Since classification accuracy of SVMs depends on kernel and penalty parameters, these parameters are tuned via an artificial immune system.

In [98] they proposed an immune multi agent recognizer model. In this model, each agent recognizer is an immune RBF neural network model. In the immune RBF neural network model, input data are regarded as antigens and the compression cluster mappings of antigens as antibodies, i.e., the hidden layer centers. The weights of the output layer can be determined by using least squares algorithm. In the immune multi agent recognizer model, each recognition subsystem possesses respective different recognizers and each agent recognizer can recognize a sort of antigen or similar antigen, so more information can be gathered.

In [99] a novel supervised algorithm based on the immune network theory, called MVINC (multiple-valued immune Network classifier), was proposed. The MVINC was applied for classification of remote sensing images. In addition, MVINC is capable of

Accepted Manuscript

ACCEPTED MANUSCRIPT

performing an immune memory using the multiple valued logic theory and immune theory for classification.

In [100] they proposed an efficient artificial immune network (EaiNet), where they combined artificial immune networks and particle swarm optimization (PSO). Particularly, they proposed algorithm uses the learning mechanism of PSO, i.e., the elite learning of each individual is capable of learning from the best in the social population. Thus, this elite learning speeds up the convergence of EaiNet.

In [101] an artificial immune system is combined with an RBF (radial basis function) artificial neural network. An immunological approach, aiNet, is used to compress the information contained in the set of data. This approach is then applied to determine the numbers and locations of the radial basis functions in an RBF neural network (RBFNN). On the other hand, in [102] a hybrid artificial immune network for optimization with swarm learning and elite-keeping is proposed.

Based on the complex and compact structure of lower extremity exoskeleton electronic system, in [103] a fault diagnosis model based on immune evolution algorithm is proposed. The design and realization method of the intelligent fault diagnosis system is also presented. According to the defects of immune algorithm that the individual diversity calculation is very complex and the vaccination is difficult, a fault calculation mechanism integrated the induction and statistic is designed, which introduced new immune operators that realized by vaccination, adjustment of diversity of every locus and immune selection. The strategies of calculating, judging and adjusting the diversity of populations by calculating the locus information entropy, the effects of control parameters, the methods of selecting and constructing a vaccine using the system information are all given.

In [104] they presented the first stages in the development of an immune inspired algorithm, via the use of a conceptual framework. Particularly, through the combination of agent based modeling and UML, they investigated the computational properties of an inherently degenerate recognition system. From their initial studies, they established that it is possible to recognize patterns using a set of degenerate receptors, and that when compared to a non-degenerate system, recognition appears quicker. In this work they accomplished the first stages in developing an immune inspired algorithm based on such properties.

In the resource limited artificial immune system (RLAIS), because the network granularity is determined by the Network Affinity Threshold (NAT) and the initialization value of NAT is obtained by calculating the distance between the antigens each other, the NAT does not reflect the network evolution process. The computation of the stimulation level at closer distance does not sufficiently reflect its advantage and is too sensitive to the change in the distance. The adoption of pure clone selection and random change operation strategy can impair the convergence of the public and the stability. By analyzing the disadvantages of RLAIS, in [105] they proposed a modified resource limited artificial immune system (MRLAIS). In MRLAIS, during the network evolution

Accepted Manuscript

ACCEPTED MANUSCRIPT

process the adaptation threshold value is computed again in each iterative to better characterize the state of affinity of the antibody at that time. A stimulation function is selected which sufficiently incarnate the advantage of the stimulation level when the antibodies distance is small and is not too sensitive to smaller distances. Finally, a resource allocation function is selected to make the network allocate the antibody more reasonably. The experimental results showed that the MRAIS had faster evolution speed and better structure stability.

In [106] they proposed a change detection algorithm called gene immune detection algorithm with complement operator. The approach decreases effectively false position appeared in previous algorithms because of gene immune detection. Also a vaccine operator and a complement operator are introduced. Therefore, the efficiency of detection is increased and the number of valid detectors is significantly decreased. The complement operator avoids the shortcoming of the Gene immune detection algorithm. Thus, detection time can be drastically decreased.

Inspired by the mechanisms of AIS, ICAIS for incremental clustering was introduced in [107]. The algorithm implements incremental clustering based on the existed clusters information. It uses the primary immune response to recognize the data belonging to the new clusters, namely the new patterns. It uses the secondary immune response to recognize the data belonging to existing clusters, i.e., old patterns.

In [108] Jerne's immune network model is extended and a new classifier based on the new immune network model and Learning Vector Quantization (LVQ) is proposed. The new classification method is called Hybrid Fuzzy Neuro-Immune Network based on Multi-Epitope approach (HFNINME). The performance of the proposed method is evaluated via several benchmark classification problems and is compared with two other immune-based classifiers. The experiments reveal that the proposed method can classify data more accurately and more efficiently.

2.2 Recent AIS applications

In this section a list of recent applications of Artificial Immune Systems is presented (see Table 3). These works have been categorized based on the particular fields and types of application with the purpose of presenting it in a summarized way. Notice that there may be an overlapping among different categories. The table is not intended to be comprehensive but rather illustrates that AISs have been used in a wide spectrum of fields.

Accepted Manuscript

ACCEPTED MANUSCRIPT

Table 3: Recent applications of AISs

Application	References
Data Mining	[128] [129]
Networking and Computer security	[96, 130] [131] [132] [88]
Optimization	[133, 134] [135] [136] [137]
Automation and Design	[138, 139] [140] [141] [142] [143]
Anomaly Detection	[144] [103]
Bioinformatics	[145] [146] [147]
Text processing	[148] [149]
Pattern Recognition, Clustering and Classification	[150, 151] [152]

3 Remarks

In reviewing recent work on artificial immune networks and the clonal selection algorithm, we observed that majority of works are applications rather than extensions and improvements of the algorithms. Some of their recent applications have been highlighted in this survey. The negative selection algorithms are continuously gaining the popularity and various variations are constantly proposed in the recent development of the AIS field. This survey found that these NSA variations are mostly concentrated on developing new detector generation scheme to improve the algorithm performance.

Research on immune inspired techniques in the future may follow many directions. One of these may be unified architecture that mimics natural defense mechanisms by integrating a set of heterogeneous immune components. On the other hand, there are some overlaps that apparently exist between AIS models and other evolutionary algorithms. For example, some well-established techniques, such as Artificial Immune Network, Clonal Selection Algorithm, and Genetic Algorithm, have the common key components, including cloning, mutation and selection. Therefore, another future efforts would be to develop distinctive immune inspired algorithms without any logical and technique overlap for any existing techniques. A greater communication among biologists, computer scientists, and engineers is needed for exploring and moving forward the AIS field.

While many other areas of the vertebrate immune systems are inspiring computer scientists and engineers to develop new algorithms, four major AIS algorithms have still been widely referred and gained popularity: 1) Negative Selection Algorithms (NSA); 2) Artificial Immune Networks (AINE); 3) Clonal lSelection Algorithms (CLONALG). 4) The Danger Theory and Dendritic Cell Algorithms (DCA). There have been many successful applications of these algorithms, such as computer security, optimization, data mining, and anomaly detection, etc.

Accepted Manuscript

ACCEPTED MANUSCRIPT

Reference:

[1] D. Dasgupta, "An overview of artificial immune systems," in *Artificial Immune Systems and Their Applications*, D. Dasgupta, Ed.: Springer-Verlag, 1998, pp. 3-19.

[2] J. Timmis, "Artificial immune systems: A novel data analysis technique inspired by the immune network theory." Aberystwyth, UK: University of Wales, 2000.

[3] L. N. D. Castro and J. Timmis, *Artificial Immune Systems: A New Computational Intelligence Approach*. London: Springer-Veralg, 2002.

[4] J. Timmis, A. Hone, T. Stibor, and E. Clark, "Theoretical advances in artificial immune systems," *Theoretical Computer Science*, vol. 403, pp. 11-32, 2008.

[5] J. Timmis, P. Andrews, N. Owens, and E. Clark, "An interdisciplinary perspective on artificial immune systems," *Evolutionary Intelligence*, vol. 1, pp. 5-26, 2008.

[6] S. Forrest, A. S. Perelson, L. Allen, and R. Cherukuri, "Self-nonself discrimination in a computer," presented at the IEEE Symposium on Research in Security and Privacy, Los Alamitos, CA, 1994.

[7] J. D. Farmer, N. H. Packard, and A. S. Perelson., "The immune system, adaptation, and machine learning," *Physica D*, vol. 22, pp. 187-204, 1986.

[8] Y. Ishida, "Fully distributed diagnosis by PDP learning algorithm: Towards immune network PDP model," presented at IEEE International Joint Conference on Neural Networks, San Diego, USA, 1990.

[9] J. Timmis, M. Neal, and J. Hunt, "An Artificial Immune System for Data Analysis," *Biosystems*, vol. 55, pp. 143-150, 2000.

[10] T. Knight and J. Timmis, "AINE: an immunological approach to data mining," presented at IEEE International Conference on Data Mining, 2001 (ICDM 2001), San Jose, CA, USA, 2001.

[11] L. N. D. Castro and F. J. V. Zuben, "The Clonal Selection Algorithm with Engineering Applications," presented at Genetic and Evolutionary Computation Conference (GECCO'00) -Workshop Proceedings, Las Vegas, Nevada, USA, 2000.

[12] L. N. d. Castro and F. J. V. Zuben, "Learning and optimization using the clonal selection principle," *IEEE Transactions on Evolutionary Computation*, vol. 6, pp. 239-251, 2002.

[13] D. Dasgupta, S. Yu, and N. S. Majumdar, "MILA - multilevel immune learning algorithm," presented at the Genetic and Evolutionary Computation Conference (GECCO 2003, Chicago, IL, USA, 2003.

[14] U. Aickelin and S. Cayzer, "The danger theory and its application to artificial immune systems," presented at The 1st International Conference on Artificial Immune Systems (ICARIS 2002), Canterbury, England, 2002.

[15] J. Greensmith, U. Aickelin, and S. Cayzer, "Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection," presented at 4th International Conference on Artificial Immune Systems (ICARIS 2005), Banff, Alberta, Canada, 2005.

[16] S. Yu and D. Dasgupta, "Conserved Self Pattern Recognition Algorithm," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

Accepted Manuscript

ACCEPTED MANUSCRIPT

[17] D. Dasgupta, N. S. Majumdar, and S. Yu, "Artificial immune systems: a bibliography," *(online)* http://www.ais.cs.memphis.edu, 2008.

[18] D. Dasgupta, *Artificial Immune Systems and Their Applications*. Berlin, Germany: Springer - Verlag, 1999.

[19] A. O. Tarakanov, V. A. Skormin, and S. P. Sokolova, *Immunocomputing: Principles and Applications*. New York: Springer, 2003.

[20] D. Dasgupta, Z. Ji, and F. Gonzalez, "Artificial immune system (AIS) research in the last five years," presented at The 2003 Congress on Evolutionary Computation, 2003. CEC '03., 2003.

[21] Y. Ishida, "Immunity-based Systems: A Design Perspective," Springer, 2004.

[22] D. Dasgupta and F. Nino, *Immunological Computation: Theory and Applications*: Auerbach Publications, 2008.

[23] S. M. Garrett, "How do we evaluate artificial immune systems?," *Evolutionary Computation*, vol. 13, pp. 145-178, 2005.

[24] J. Kim, P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection – a review," *Natural Computing*, vol. 6, pp. 413-466, 2007.

[25] E. Hart and J. Timmis, "Application areas of AIS: The past, the present and the future," *Applied Soft Computing*, vol. 8, pp. 191-201, 2008.

[26] F. Freschi, C. A. C. Coello, and M. Repetto, "Multiobjective Optimization and Artificial Immune Systems: A Review," in *Handbook of Research on Artificial Immune Systems and Natural Computing: Applying Complex Adaptive Technologies, Medical Information Science Reference*, H. Mo, Ed. Hershey, New York, 2009, pp. 1-21.

[27] Z. Ji and D. Dasgupta, "Revisiting Negative Selection Algorithms," *Evolutionary Computation*, vol. 15, pp. 223-251, 2007.

[28] X. Z. Gao, S. J. Ovaska, and X. Wang, "Genetic Algorithms-based Detector Generation in Negative Selection Algorithm," presented at 2006 IEEE Mountain Workshop on Adaptive and Learning Systems, 2006.

[29] X. Z. Gao, S. J. Ovaska, X. Wang, and M.-Y. Chow, "Clonal Optimization of Negative Selection Algorithm with Applications in Motor Fault Detection," presented at IEEE International Conference on Systems, Man and Cybernetics, 2006. SMC '06., Taipei, 2006.

[30] J. M. Shapiro, G. B. Lamont, and G. L. Peterson, "An evolutionary algorithm to generate hyper-ellipsoid detectors for negative selection," presented at the 2005 conference on Genetic and evolutionary computation, Washington DC, USA, 2005.

[31] M. Ostaszewski, F. Seredynski, and P. Bouvry, "Immune anomaly detection enhanced with evolutionary paradigms," presented at the 8th annual conference on Genetic and evolutionary computation (GECCO 2006), Seattle, Washington, USA, 2006.

[32] M. Ostaszewski, F. Seredynski, and P. Bouvry, "Coevolutionary-based Mechanisms for Network Anomaly Detection," *Journal of Mathematical Modelling and Algorithms*, vol. 6, pp. 411-431, 2007.

[33] W. Luo, X. Wang, Y. Tan, and X. Wang, "A Novel Negative Selection Algorithm with an Array of Partial Matching Lengths for Each Detector," presented at 9th

Accepted Manuscript

International Conference on Parallel Problem Solving from Nature - PPSN IX, 2006.

[34] W. Luo, Z. Zhang, and X. Wang, "A heuristic detector generation algorithm for negative selection algorithm with hamming distance partial matching rule," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

[35] W. Luo, X. Wang, and X. Wang, "A novel fast negative selection algorithm enhanced by state graphs," presented at 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos, Brazil, 2007.

[36] W. Luo, J. Wang, and X. Wang, "Evolutionary Negative Selection Algorithms for Anomaly Detection," presented at 8th Joint Conference on Information Science (JCIS 2005), Salt Lake City, Utah, USA, 2005.

[37] W. Luo, P. Guo, and X. Wang, "On convergence of Evolutionary Negative Selection Algorithms for anomaly detection," presented at IEEE Congress on Evolutionary Computation, 2008. CEC 2008. (IEEE World Congress on Computational Intelligence), Hong Kong, China, 2008.

[38] B. Xu, W. Luo, X. Pei, M. Zhang, and X. Wang, "On Average Time Complexity of Evolutionary Negative Selection Algorithms for Anomaly Detection," presented at the 2009 World Summit on Genetic and Evolutionary Computation (2009 GEC Summit),, Shanghai, China, 2009.

[39] Y. Zhanga, W. Luo, Z. Zhang, B. Li, and X. Wang, "A hardware/software partitioning algorithm based on artificial immune principles," *Applied Soft Computing*, vol. 8, pp. 383-391, 2008.

[40] W. Ma, D. Tran, and D. Sharma, "Negative Selection with Antigen Feedback in Intrusion Detection," presented at the 7th international conference on Artificial Immune Systems, Phuket, Tailand, 2008.

[41] A. Chmielewski and S. T. Wiezchon, "V-Detector algorithm with tree-based structures," presented at the International Multiconference on Computer Science and Information Technology, 2006.

[42] K. Ciesielski, S. T. Wierzchon, and M. A. Klopotek, "An Immune Network for Contextual Text Data Clustering," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

[43] T. Stibor, P. Mohr, J. Timmis, and C. Eckert, "Is negative selection appropriate for anomaly detection?," presented at the 2005 conference on Genetic and evolutionary computation (GECCO 2005), Washington DC, USA, 2005.

[44] Z. Ji and D. Dasgupta, "Real-valued negative selection using valuable-sized detectors," presented at Genetic and Evolutionary Computation Conference (GECCO 2004), Seattle, WA, USA, 2004.

[45] T. Stibor, J. Timmis, and C. Eckert, "Generalization regions in hamming negative selection," in *Intelligent Information Processing and Web Mining*, vol. 35, *Advances in Soft Computing*: Springer Berlin / Heidelberg, 2006, pp. 447-456.

[46] T. Stibor, J. Timmis, and C. Eckert, "On Permutation Masks in Hamming Negative Selection," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

Accepted Manuscript

[47] T. Stibor, "Phase Transition and the Computational Complexity of Generating r - Contiguous Detectors," presented at 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos, Brazil, 2007.

[48] T. Stibor, "An empirical study of self/non-self discrimination in binary data with a kernel estimator," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[49] B. Caldas, M. Pita, and F. Buarque, "How to Obtain Appropriate Executive Decisions Using Artificial Immunologic Systems," presented at 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos, Brazil, 2007.

[50] A. J. Graaff and A. P. Engelbrecht, "Optimized Coverage of Non-self with Evolved Lymphocytes in an Artificial Immune System," *International Journal of Computational Intelligence Research (IJCIR)*, vol. 2, pp. 127-150, 2006.

[51] J. L. M. Amaral, J. F. M. Amaral, and R. Tanscheit, "Real-Valued Negative Selection Algorithm with a Quasi-Monte Carlo Genetic Detector Generation," presented at 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos, Brazil, 2007.

[52] W. J. Morokoff and R. E. Caflisch, *Quasi-Monte Carlo Integration*: Academic Press, 1993.

[53] G. Levy, "Where Numerics Matter: Matter: An introduction to quasi-random numbers," *Financial Engineering News*, 2002.

[54] J. Pacheco and J. F. Costa, "The Abstract Immune System Algorithm," presented at the 6th International Conference on Unconventional Computation, Kingston, Canada, 2007.

[55] H. Schmidtchen and U. Behn, "Randomly evolving idiotypic networks: analysis of building principles," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

[56] M. Brede and U. Behn, "Patterns in randomly evolving networks: idiotypic networks," *Phys Rev E Stat Nonlin Soft Matter Phys*, vol. 67, pp. 031920, 2003.

[57] G. P. Coelho and F. J. V. Zuben, "omni-aiNet: An Immune-Inspired Approach for Omni Optimization," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

[58] G. P. Coelho, F. O. d. França, and F. J. V. Zuben, "A Multi-Objective Multipopulation Approach for Biclustering," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[59] A. Secker, M. N. Davies, A. A. Freitas, J. Timmis, E. Clark, and D. R. Flower, "An Artificial Immune System for Evolving Amino Acid Clusters Tailored to Protein Function Prediction," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[60] J. Cui, L. Y. Han, H. Li, C. Y. Ung, Z. Q. Tang, C. J. Zheng, Z. W. Cao, and Y. Z. Chen, "Computer prediction of allergen proteins from sequence-derived protein structural and physicochemical properties," *Mol Immunol*, vol. 44, pp. 514-20, 2007.

[61] A. Christopoulos and T. Kenakin, "G protein-coupled receptor allosterism and complexing," *Pharmacol Rev*, vol. 54, pp. 323-74, 2002.

[62] R. S. Takehara and R. Romero, "Artificial Immune Systems Applied to Optimal Capacitor Placement in Radial Distribution Networks," presented at 2006 IEEE

Accepted Manuscript

ACCEPTED MANUSCRIPT

PES Transmission and Distribution Conference and Exposition: Latin America, 2006. TDC '06. IEEE/PES, Caracas, Venezuela, 2006.

[63] T. Stibor and J. Timmis, "An Investigation on the Compression Quality of aiNet," presented at IEEE Symposium on Foundations of Computational Intelligence, 2007. FOCI 2007, 2007.

[64] A. Ciccazzo, P. Conca, G. Nicosia, and G. Stracquadanio, "An Advanced Clonal Selection Algorithm with Ad Hoc Network-Based Hypermutation Operators for Synthesis of Topology and Sizing of Analog Electrical Circuits," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[65] R. Halavati, S. B. Shouraki, M. J. Heravi, and B. J. Jashmi, "An artificial immune system with partially specified antibodies," presented at the 9th annual conference on Genetic and evolutionary computation (GECCO 2007), London, England, 2007.

[66] P. May, J. Timmis, and K. Mander, "Immune and Evolutionary Approaches to Software Mutation Testing," presented at 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos, Brazil, 2007.

[67] V. Cutello, G. Nicosia, M. Pavone, and J. Timmis, "An Immune Algorithm for Protein Structure Prediction on Lattice Models," *IEEE Transactions on Evolutionary Computation*, vol. 11, pp. 101-117, 2007.

[68] W. O. Wilson, P. Birkin, and U. Aickelin, "Price Trackers Inspired by Immune Memory," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

[69] P. Matzinger, "The danger model: a renewed sense of self," *Science*, vol. 296, pp. 301-5, 2002.

[70] P. Bretscher and M. Cohn, "A theory of self-nonself discrimination," *Science*, vol. 169, pp. 1042-9, 1970.

[71] P. Matzinger, "Tolerance, danger, and the extended family," *Annu Rev Immunol*, vol. 12, pp. 991-1045, 1994.

[72] J. Greensmith, U. Aickelin, and J. Twycross, "Detecting Danger: Applying a Novel Immunological Concept to Intrusion Detection Systems'," presented at 6th International Conference in Adaptive Computing in Design and Manufacture (ACDM 2004 Poster), Bristol, UK, 2004.

[73] C. E. Prieto, F. Nino, and G. Quintana, "A goalkeeper strategy in robot soccer based on Danger Theory," presented at IEEE Congress on Evolutionary Computation, 2008. CEC 2008. (IEEE World Congress on Computational Intelligence). Hong Kong, 2008.

[74] A. Iqbal and M. A. Maarof, "Danger Theory and Intelligent Data Processing," presented at World Academy of Science, Engineering and Technology, 2005.

[75] A. Secker, A. Freitas, and J. Timmis, "Towards a danger theory inspired artificial immune system for web mining," in *Web Mining: applications and techniques*, A. Scime, Ed.: Idea Group, 2005, pp. 145-168.

[76] R. Steinman and Z. Cohn, "Identification of a novel cell type in peripheral lymphoid organs mice," *The journal of Experimental Medicine*, vol. 137, pp. 1142-1162, 1973.

[77] M. L. Kapsenberg, "Dendritic-cell control of pathogen-driven T-cell polarization," *Nat Rev Immunol*, vol. 3, pp. 984-93, 2003.

Accepted Manuscript

ACCEPTED MANUSCRIPT

[78] T. Jamie and U. Aickelin, "Towards a conceptual framework for innate immunity," presented at 3rd International Conference on Artificial Immune Systems (ICARIS 2004), Catania, Italy, 2004.

[79] K. W. Yeom, "Immune-inspired Algorithm for Anomaly Detection. I," in *Computational Intelligence in Information Assurance and Security*, vol. 57, *Studies in Computational Intelligence*. Heidelberg: Springer, 2007, pp. 129-154.

[80] J. Greensmith, U. Aickelin, and J. Twycross, "Articulation and Clarification of the Dendritic Cell Algorithm," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

[81] F. Gu, J. Greensmith, and U. Aickelin, "Further Exploration of the Dendritic Cell Algorithm: Antigen Multiplier and Time Windows," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[82] R. Oates, J. Greensmith, U. Aickelin, J. Garibaldi, and G. Kendall, "The Application of a Dendritic Cell Algorithm to a Robotic Classifier," presented at 6th International Conference on Artificial Immune Systems (ICARIS 2007), Santos, Brazil, 2007.

[83] J. Greensmith and U. Aickelin, "The deterministic dendritic cell algorithm," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[84] S. Manzoor, M. Z. Shafiq, S. M. Tabish, and M. Farooq, "A Sense of ‘Danger’ for Windows Processes," presented at 8th International Conference on Artificial Immune Systems, ICARIS 2009, York, UK, 2009.

[85] J. Kim, P. Bentley, C. Wallenta, M. Ahmed, and S. Hailes, "Danger Is Ubiquitous: Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm," presented at 5th International Conference on Artificial Immune Systems (ICARIS 2006), Oeiras, Portugal, 2006.

[86] J. Greensmith and U. Aickelin, "Dendritic cells for SYN scan detection," presented at the 9th annual conference on Genetic and evolutionary computation (GECCO 2007), London, England, 2007.

[87] J. Greensmith, U. Aickelin, and G. Tedesco, "Information fusion for anomaly detection with the dendritic cell algorithm," *Information Fusion*, vol. 11, pp. 21-34, 2010.

[88] N. Mazhar and M. Farooq, "A sense of danger: dendritic cells inspired artificial immune system for manet security," presented at the 10th annual conference on Genetic and evolutionary computation (GECCO 2008), Atlanta, GA, USA, 2008.

[89] U. Aickelin and J. Greensmith, "Sensing Danger: Innate Immunology for Intrusion Detection," The University of Nottingham, Nottingham, UK 2007.

[90] W. Wang, S. Gao, and Z. Tang, "A Complex Artificial Immune System," presented at the 2008 Fourth International Conference on Natural Computation, 2008.

[91] P. A. D. Castro and F. J. V. Zuben, "MOBAIS: A Bayesian Artificial Immune System for Multi-Objective Optimization," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[92] P. A. D. Castro and F. J. V. Zuben, "BAIS: A Bayesian Artificial Immune System for the Effective Handling of Building Blocks," *Information Sciences*, vol. 179, pp. 1426-1440, 2009.

Accepted Manuscript

[93] P. A. D. Castro and F. J. V. Zuben, "Feature Subset Selection by Means of a Bayesian Artificial Immune System," presented at Eighth International Conference on Hybrid Intelligent Systems, 2008. HIS '08., Barcelona, 2008.

[94] P. A. D. Castro and F. J. V. Zuben, "Multi-objective Feature Selection Using a Bayesian Artificial Immune System," *International Journal of Intelligent Computing and Cybernetics*, vol. 3, pp. 235-256, 2010.

[95] P. A. D. Castro and F. J. V. Zuben, "Multi-objective Bayesian Artificial Immune System: Empirical Evaluation and Comparative Analyses," *Journal of Mathematical Modelling and Algorithms*, vol. 8, pp. 151-173, 2009.

[96] B. Chen and C. Zang, "Unsupervised Structure Damage Classification Based on the Data Clustering and Artificial Immune Pattern Recognition," presented at 8th International Conference on Artificial Immune Systems, ICARIS 2009, York, UK, 2009.

[97] I. Aydin, M. Karakose, and E. Akin, "Artificial immune based support vector machine algorithm for fault diagnosis of induction motors," presented at International Aegean Conference on Electrical Machines and Power Electronics, 2007. ACEMP apos;07, 2007.

[98] Z. Qiu, Y. Zhou, J. Wang, P. Zhang, and Z. Liu, "Study on Multi Agent Recognizer Model Based on Immune RBF Neural Network," presented at IEEE International Conference on Control and Automation, 2007. ICCA 2007., 2007.

[99] Y. Zhong, L. Zhang, J. Gong, and P. Li, "A Supervised Artificial Immune Classifier for Remote-Sensing Imagery," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 45, pp. 3957-3966, 2007.

[100] Z. Li, Y. Zhang, and H.-Z. Tan, "An Efficient Artificial Immune Network with Elite-Learning," presented at Third International Conference on Natural Computation, 2007. ICNC 2007., 2007.

[101] J. Deng, Y. Jiang, and Z. Mao, "An Artificial Immune Network Approach for Pattern Recognition," presented at Third International Conference on Natural Computation, 2007. ICNC 2007, 2007.

[102] J. Fu, z. Li, and H.-Z. Tan, "A Hybrid Artificial Immune Network with Swarm Learning," presented at International Conference on Communications, Circuits and Systems, 2007. ICCCAS 2007, 2007.

[103] H. Yang, M. Elhadef, A. Nayak, and X. Yang, "Network Fault Diagnosis: An Artificial Immune System Approach," presented at 14th IEEE International Conference on Parallel and Distributed Systems, 2008. ICPADS '08., 2008.

[104] M. Mendao, J. Timmis, P. S. Andrews, and M. Davies, "The Immune System in Pieces: Computational Lessons from Degeneracy in the Immune System," presented at IEEE Symposium on Foundations of Computational Intelligence, 2007. FOCI 2007., Honolulu, HI, 2007.

[105] T. Liu, Z. Hu, Y. Zhou, and Z. Wang, "A Modified Resource Limited Artificial Immune System," presented at 2008 International Symposium on Electronic Commerce and Security, 2008.

[106] Y.-J. Zhang and S.-H. Wu, "A Gene Immune Detection Algorithm with Complement Operator on the Basis of Biological Immune Principles," presented at International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP apos;08, 2008.

Accepted Manuscript

ACCEPTED MANUSCRIPT

[107] X. Li, T. Lu, Z. Wang, and C. Gao, "ICAIS: A Novel Incremental Clustering Algorithm Based on Artificial Immune Systems," presented at 2008 International Conference on Internet Computing in Science and Engineering, 2008.

[108] H. Izadinia, F. Sadeghi, and M. M. Ebadzadeh, "A Hybrid Fuzzy Neuro-Immune Network based on Multi-Epitope approach," presented at 2009 International Joint Conference on Neural Networks, Atlanta, Ga, USA, 2009.

[109] F. M. Burnet, *The clonal selection theory of acquired immunity*: Nashville, Vanderbilt University Press, 1959.

[110] C. A. Janeway, Jr., "Approaching the asymptote? Evolution and revolution in immunology," *Cold Spring Harb Symp Quant Biol*, vol. 54 Pt 1, pp. 1-13, 1989.

[111] N. K. Jerne, "Towards a network theory of the immune system," *Ann Immunol (Paris)*, vol. 125C, pp. 373-89, 1974.

[112] J. E. Hunt and D. E. Cooke, "Learning using an artificial immune system," *Journal of Network and Computer Applications*, vol. 19, pp. 189-212, 1996.

[113] 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*, D. Dasgupta, Ed.: Springer-Verlag, 1999, pp. 157-184.

[114] J. Timmis and M. Neal, "A resource limited artificial immune system for data analysis," *Knowledge Based System*, vol. 14, pp. 121-130, 2001.

[115] E. Hart and P. Ross, "Exploiting the analogy between immunology and sparse distributed memories: A system for clustering non-stationary data," presented at the 1st International Conference on Artificial Immune Systems (ICARIS 2002), University of Kent at Canterbury, 2002.

[116] T. Knight and J. Timmis, "A multi-layered immune inspired approach to data mining," presented at the 4th International Conference on Recent Advances in Soft Computing, Nottingham, UK, 2002.

[117] O. Nasraoui, D. Dasgupta, and F. Gonzalez, "A novel artificial immune system approach to robust data mining," presented at the International Conference on Genetic and Evolutionary Computation (GECCO 2002), New York, 2002.

[118] O. Nasraoui, F. Gonzalez, C. Cardona, C. Rojas, and D. Dasgupta, "A scalable artificial immune system model for dynamic unsupervised learning," presented at the Genetic and Evolutionary Computation Conference (GECCO 2003, Chicago, IL, USA, 2003.

[119] O. Nasraoui, F. Gonzalez, and D. Dasgupta, "The fuzzy ais: Motivations, basic concepts, and applications to clustering and web profiling," presented at IEEE International Conference on Fuzzy Systems, Hawaii, 2002.

[120] M. Neal, "An artificial immune system for continuous analysis of time-varying data," presented at the 1st International Conference on Artificial Immune Systems (ICARIS 2002), University of Kent at Canterbury, 2002.

[121] A. Watkins and J. Timmis, "Artificial immune recognition system (AIRS): Revisions and refinements," presented at the 1st International Conference on Artificial Immune Systems (ICARIS 2002), University of Kent at Canterbury, 2002.

[122] A. B. Watkins and L. C. Boggess, "A resource limited artificial immune classifier," presented at IEEE World Congress on Computational

Accepted Manuscript

Intelligence/proceedings of the special sessions on artificial immune systems in the 2002 Congress on Evolutionary Computation, Honolulu, Hawaii, 2002.

[123] S. Wierzchon and U. Kuzelewska, "Stable clusters formation in an artificial immune system," presented at the 1st International Conference on Artificial Immune Systems (ICARIS 2002), University of Kent at Canterbury, 2002.

[124] L. N. d. Castro and F. J. V. Zuben, "aiNet: An artificial immune network for data analysis," in *Data Mining: A Heuristic Approach*, H. A. Abbass, R. A. Sarker, and C. S. Newton, Eds.: Idea Group Publishing, USA, 2001, pp. 231-259.

[125] L. N. d. Castro and J. Timmis, "An artificial immune network for multimodal optimization," presented at 2002 Congress on Evolutionary Computation (CEC 2002). Part of the 2002 IEEE World Congress on Computational Intelligence, Honolulu, Hawaii, USA, 2002.

[126] C. A. Janeway, Jr., "The immune system evolved to discriminate infectious nonself from noninfectious self," *Immunol Today*, vol. 13, pp. 11-6, 1992.

[127] J. P. Twycross, "Integrated Innate and Adaptive Artificial Immune Systems applied to Process Anomaly Detection.," in *School of Computer Science*. Nottingham: University of Nottingham, U.K., 2007.

[128] S. Golzari, S. Doraisamy, M. N. B. Sulaiman, N. I. Udzir, and N. M. Norowi, "Artificial Immune Recognition System with Nonlinear Resource Allocation Method and Application to Traditional Malay Music Genre Classification," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[129] M. Puteh, A. R. Hamdan, K. Omar, and A. A. Bakar, "Flexible Immune Network Recognition System for Mining Heterogeneous Data," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[130] D. Dal, S. Abraham, A. Abraham, S. Sanyal, and M. Sanglikar, "Evolution Induced Secondary Immunity: An Artificial Immune System Based Intrusion Detection System," presented at the 2008 7th Computer Information Systems and Industrial Management Applications, 2008.

[131] M. Z. Shafiq, S. A. Khayam, and M. Farooq, "Improving accuracy of immune-inspired malware detectors by using intelligent features," presented at the 10th annual conference on Genetic and evolutionary computation (GECCO 2008), Atlanta, GA, USA, 2008.

[132] J. Zhang and Y. Liang, "A Novel Intrusion Detection Model Based on Danger Theory," presented at Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 2008. PACIIA '08., Wuhan, China, 2008.

[133] M. Gong, L. Jiao, H. Du, and L. Bo, "Multiobjective Immune Algorithm with Nondominated Neighbor-Based Selection," *Evolutionary Computation*, vol. 16, pp. 225-255, 2008.

[134] T. A. S. Masutti and L. N. d. Castro, "A Neuro-Immune Algorithm to Solve the Capacitated Vehicle Routing Problem," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[135] I. N. Vieira, B. S. L. P. d. Lima, and B. P. Jacob, "Optimization of Steel Catenary Risers for Offshore Oil Production Using Artificial Immune System," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

Accepted Manuscript

ACCEPTED MANUSCRIPT

[136] L. M. Honório, M. Vidigal, and L. E. Souza, "Dynamic Polymorphic Agents Scheduling and Execution Using Artificial Immune Systems," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[137] H. Yu, "Optimizing task schedules using an artificial immune system approach," presented at the 10th annual conference on Genetic and evolutionary computation (GECCO 2008), Atlanta, GA, USA, 2008.

[138] W. W. Godfrey and S. B. Nair, "An Immune System Based Multi-robot Mobile Agent Network," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[139] A. Ko, H. Y. K. Lau, and N. M. Y. Lee, "AIS Based Distributed Wireless Sensor Network for Mobile Search and Rescue Robot Tracking," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[140] Y. Liu, J. Timmis, and T. Clarke, "A Neuro-Immune Inspired Robust Real Time Visual Tracking System," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[141] A. Whitbrook, U. Aickelin, and J. Garibaldi, "An Idiotypic Immune Network as a Short-Term Learning Architecture for Mobile Robots," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[142] M. Chen, Y. Chen, and Z. Yao, "A Virtual and Real HCI System Based on Artificial Immune System," presented at the 2008 Second International Conference on Genetic and Evolutionary Computing, 2008.

[143] L. Xuepeng, "Immune PI control on PMSM speed regulating system," presented at 7th World Congress on Intelligent Control and Automation, 2008. WCICA 2008., Chongqing, China, 2008.

[144] M. F. A. Gadi, X. Wang, and A. P. d. Lago, "Credit Card Fraud Detection with Artificial Immune System," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[145] W. Wilson, P. Birkin, and U. Aickelin, "The motif tracking algorithm," *International Journal of Automation and Computing*, vol. 5, pp. 32-44, 2008.

[146] S. Jung, K.-i. Cho, and D. Lee, "AIS-Based Bootstrapping of Bayesian Networks for Identifying Protein Energy Route," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[147] C. Chen, C. Xu, R. Bie, and X. Z. Gao, "Artificial Immune Recognition System for DNA Microarray Data Analysis," presented at the 2008 Fourth International Conference on Natural Computation, 2008.

[148] A. Abi-Haidar and L. M. Rocha, "Adaptive Spam Detection Inspired by a Cross-Regulation Model of Immune Dynamics: A Study of Concept Drift," presented at 7th International Conference on Artificial Immune Systems, Phuket, Thailand, 2008.

[149] L. Albergante, "Wireless discussion forums: Automatic management via artificial immune systems," presented at International Symposium on Performance Evaluation of Computer and Telecommunication Systems, 2008. SPECTS 2008., 2008.

[150] C.-M. Wang, C.-T. Kuo, C.-Y. Lin, and G.-H. Chang, "Application of Artificial Immune System Approach in MRI Classification," *EURASIP Journal on*

Accepted Manuscript

ACCEPTED MANUSCRIPT

Advances in Signal Processing, vol. 2008, pp. Article ID 547684, 8 pages, 2008. doi:10.1155/2008/547684, 2008.

[151] H. Zheng, D. Jiaying, Z. Liu, and Y. Wang, "Research on Vehicle Image Classifier Based on Concentration Regulating of Immune Clonal Selection," presented at the 2008 Fourth International Conference on Natural Computation, 2008.

[152] H. Li, C. Wang, and A. Wang, "Medical Image Registration Based on More Features and Artificial Immune Algorithm," presented at 2009 International Joint Conference on Artificial Intelligence, Hainan Island, China, 2009.

Accepted Manuscript