A Review of Artificial Immune Systems

Zafer Ataser
Kuzey Kıbrıs Turkcell, Bedreddin Demirel Avenue Salih Mecit Street Lefkosa, TRNC, Mersin 10, Turkey

Keywords: Artificial Immune Systems, Immune Network Theory, Clonal Selection, Danger Theory, Negative Selection Algorithm.

Abstract: Artificial Immune Systems (AIS) are class of computational intelligent methods developed based on the principles and processes of the biological immune system. AIS methods are categorized mainly into four types according to the inspired principles and processes of immune system. These categories are clonal selection, negative selection, immune network and danger theory. This paper reviews the models of AIS and the progress of them. The fundamental characteristics of AIS models are identified and some major studies of each model are given. In addition to that, some application areas of AIS models are explained.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

1 INTRODUCTION

Inspiration for computational methods has often come from analogy with biological phenomena. The biological immune system is one of them, and researches inspired by the biological immunity caused the emergence of a new area, Artificial Immune System (AIS), for computational intelligence.

The biological immune system is still an active research area for the biology discipline, and as a result of the researches, many theories have been proposed about the mechanism of the biological immune system. Hence, various models of AIS were developed inspired by the different biological immune theories. Garret (Garrett, 2005) present these models as immune network, clonal selection, negative selection and danger theory.

The immune system constitutes of two main mechanisms, innate immunity and adaptive (acquired) immunity. The innate immunity is the first layer defense mechanism, and the second one is the adaptive immunity. The innate immunity consists of basic elements the organism is born with such as skin and physical barriers. The adaptive immunity provides the ability to adapt over time to recognize specific pathogens, and it creates immunological memory after an initial response to a specific pathogen. The clonal selection theory was developed to describe the principles of adaptive immunity. The main features of the clonal selection theory are (de Castro and Zuben, 2002):

- Clone activated mature cells and generates random changes on clone cells with high rates (somatic mutation);
- Elimination of newly differentiated cells which match self cells;
- proliferation and differentiation on activation of cells by antigens.

The immune network theory was developed to explain the adaptive immune system mechanism, and it had been introduced by Jerne (Jerne, 1974). The theory states that the immune system maintains an idiotypic network of interconnected B cells for antigen recognition. These cells interact with each other, and they interconnect with each other in definite rules to stabilize the network. Two interacting cells are connected if their affinities exceed a certain threshold. The strength of the connection is directly proportional to their affinity (Al-Enezi et al., 2010).

The biological negative selection describes T cells maturation process in thymus called T cell tolerance. T cell's gene segments are randomly rearranged together by somatic gene rearrangement, and bases are inserted to create T cell against antigens. The generated cells are eliminated when they recognize self cells as antigens. In the end of this elimination process, the remaining cells, mature cells, are released from the thymus. In this manner, these mature cells increase the ability of the immune system to detect unknown antigens. Inspired by the biological negative selection, the process of negative selection generates a set of T-cell detectors that can detect any form of non-self in AIS (Garrett, 2005).

The main idea of danger theory states that the im-

Ataser Z..
A Review of Artificial Immune Systems.
DOI: 10.5220/0004553101280135
In *Proceedings of the 5th International Joint Conference on Computational Intelligence* (ECTA-2013), pages 128-135
ISBN: 978-989-8565-77-8
Copyright © 2013 SCITEPRESS (Science and Technology Publications, Lda.)

mune system responds to danger instead of non-self (Matzinger, 2002). Danger theory fundamentally accepts the need for discrimination as other theories. On the other, the difference between danger theory and others is the answer to what should be responded to. Danger theory responds danger instead of foreignness, and danger is evaluated by damage to cells specified by distress signals. These signals are sent out in case of an unnatural death of cells.

2 MAJOR AIS WORKS

Artificial Immune System (AIS) attracted the attention of researchers after the first studies, and many researches have been done on it. AIS emerged as a new branch of Artificial Intelligence (AI) as other disiplines inspired from biological mechanisms. There are many studies on AIS, and some of them focused on the categorization of the proposed AIS methods based on their porperties (Garrett, 2005),(Al-Enezi et al., 2010). This section reviews the studies on existing models.

2.1 Immune Network Theory

Timmis et al. (Timmis et al., 2000), (Timmis and Neal, 2001) introduced Artificial Immune Network (AINE) method which uses artificial recognition ball (ARB) to represent a number of identical B cells described in immune network. The stimulated B cells are subjected to clone and somatic hypermutation ensures that these clones are differentiated a relatively large proportion of the parent cell. The cells stimulated by particular antigen are kept in the immunological memory for that antigen. Two B cells are connected based on the affinity between them. The affinity is measured using the Euclidean distance between the two B cells. The two B cells are connected when the affinity between them exceeds the network affinity threshold. The connected B cells are called as ARB. Timmis et al. (Timmis and Neal, 2001) were tested AINE using Fisher Iris dataset, and AINE generates the disconnected clusters which provide the variety which allows the immune system to generalize variations in the data encountered.

Castro and Zuben (de Castro and Zuben, 2001) proposed "Artificial Immune Network Model for Data Analysis" (aiNet) learning algorithm. This algorithm uses nodes simulating antibodies, while AINE uses nodes inspired by B cells. Antibodies are receptor molecules that are secreted B cells with the primary role recognizing and binding with an antigen. One of the important aims of this algorithm is to increase the generalization of antibodies and the network. In order to do that, aiNet suppresses antibodies with low antigenic and high affinities according to the suppression threshold. There are two suppressive steps in this algorithm, clonal suppression and network suppression. Hence, the suppression threshold controls the specificity level of the antibodies, the clustering accuracy and network plasticity. aiNet provides the reconstruction of the metric and topological relationships. Reproducing the topological relationships causes that similar information are mapped onto closer antibodies, eventually the same one and clustering of the input space.

Liu and Xu (Liu and Xu, 2008) introduced a cooperative artificial immune network called CoAIN to improve search ability and search speed. The CoAIN uses cooperative strategy inspired by particle swarm behavior. This means that each network cell has the ability to cooperate with other individuals, and this cooperation adjusts position according to its own experience and the experience of the best cell. In this way, this cooperation ability finds the best position encountered by itself and its neighbor. In the other feature of CoAIN, antibodies with fitness dominate clonal selection, and smaller step size of mutation is used in clonal selection to find global optimization. Step size of mutation is decreased smoothly with the increase of generation to fit for finer search. This paper shows that some basic immune principles together with simple cooperation behavior makes possible to solve complex optimization tasks.

Coelho and Zuben (Coelho and Zuben, 2010) proposed Concentration-based Artificial Immune Network (cob-aiNet) to solve single optimization problems, and they (Coelho and Zuben, 2011) introduce the extension of cob-aiNet to solve multi-objective optimization problems. The cob-aiNet exploits the features of a concentration-based immune model. Thus, it controls the dynamics of the population, and uses new mechanisms to stimulate and maintain the diversity of the individuals in the population.

Zhong and Zhang (Zhong and Zhang, 2012) present a novel supervised algorithm based on the immune network theory, the artificial antibody network (ABNet). In this method, every antibody consists of two important attributes, its center vector and recognizing radius. The antibody can recognize all antigens within the range of its recognizing radius. ABNet was designed for classifications of multi-/hyperspectral remote sensing images.

2.2 Clonal Selection

Castro and Zuben (de Castro and Zuben, 1999), (de Castro and Zuben, 2000) popularized the artificial form of clonal selection developing an algorithm called clonal selection algorithm (CSA). They applied CSA to different problems and compared it with the standard genetic algorithm (GA) (de Castro and Zuben, 2000). Then, they (de Castro and Zuben, 2002) modified the algorithm and renamed it to CLONALG, which is the most known clonal selection algorithm. Two forms of CLONALG were introduced, one for optimization tasks and one for pattern matching. CLONALG takes into account the following main immune features;

- maintenance of a specific memory set;
- selection and cloning of the most stimulated antibodies;
- death of nonstimulated antibodies;
- affinity maturation
- reselection of the clones according to their antigenic affinity, generation, and maintenance of diversity.

Brownlee (Brownlee, 2005) introduced Clonal Selection Classification Algorithm (CSCA) which is mainly based on CLONALG. Concern of CSCA increases classification accuracy. CSCA is considered as a function optimization procedure that maximizes the number of correctly classified patterns and minimizes the number of misclassified patterns. The algorithm is constituted of four main steps:

1. Initialization - Initialize the antibody population.
2. Training looping - Involve selection and pruning step, cloning and mutation step and the insertion the generated clones.
3. Final Pruning - Prepare fitness scores and perform pruning
4. Classification - Classify using the antibody population.

Oliveira et al. (L. O. V. B. Oliveira, 2012) proposed Clonal Selection Classifier with Data Reduction (CSCDR) which is mainly based on the CSCA. CSCA is modified to increase the performance and to decrease the number of memory cells. The mutation process is changed to get better results in search space process, and a control parameter is inserted to decrease the number of memory cells produced.

Li et al. (Li et al., 2012) introduced Reconfigurable Space Clone Selection Algorithm (RSCSA), which is focuses on the antibody population size and antibody search space. RSCSA reduces the search space and antibody population size. Due to this reduction, the algorithm has strong robustness and fast convergent speed.

2.3 Danger Theory

Aickelin and Cayzer (Aickelin and Cayzer, 2002) presented the one of the first major studies about the danger theory from AIS perspective. This study explains Matzinger's Danger Theory in the first part. Then, the danger theory is evaluated from the perspective of AIS practitioners. In this evaluation, the danger concept is discussed, and the danger theory is compared with the other AIS models, i.e. negative selection. Beside this, they debate about how to implement the danger theory based on the AIS perspective. In the last section, the AIS applications are evaluated based on the danger theory.

Greensmith et al. (Greensmith et al., 2004) described the danger theory and AIS applications. The current state of intrusion detection systems (IDS) was presented. They discussed the application of the danger theory on IDS, and claimed that significant improvements will be provided. Kim et al.(Kim et al., 2005) and Roper (Roper, 2009) also proposed that the danger theory is more suitable than other AIS models to apply on IDS.

Aickelin and Greensmith (Aickelin and Greensmith, 2007) introduced two algorithms, the Dendritic Cell Algorithm (DCA) and the Toll-like Receptor algorithm (TLR), developed based on the danger theory. These algorithms were developed inspired by different aspects of the danger theory. DCA and TLR proved that it is possible to build feasible AIS algorithms based on the principles of the danger theory.

Zhu and Tan (Zhu and Tan, 2011) proposed a danger theory based learning (DTL) model, which mimic the mechanism of the danger theory. The algorithm was tested with spam filtering problem and compared with classical machine learning approaches, Support Vector Machine (SVM) and Naive Bayes (NB). In experiments, the DTL model outperformed SVM, NB.

2.4 Negative Selection Algorithm (NSA)

Artificial Immune System (AIS) covers many models inspired by the biological immune system. The first model, negative selection algorithm (NSA), among AIS models was introduced by Forrest et al. (Forrest et al., 1994). Many researches have been performed after the introduction of NSA. These researches proposed various NSA, and they are differentiated in data representation, detector representation, self definition and matching rule.

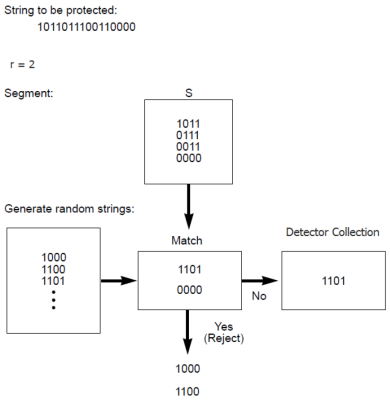

Figure 1: Generation of valid detector set (Forrest et al., 1994).

Forrest et al. (Forrest et al., 1994) proposed NSA inspired by discrimination between self and non-self in immune system. Therefore, NSA imitates the T cell maturation process, which gives the ability to T cells to make discrimination between self and non-self. To implement NSA, there are some critical development considerations; data representation, self definition, detector coverage, matching rule. This study converts the given data to binary representation, so detectors are also represented in binary form. Self was defined as the string to be protected, and other (non-self) to be any other string. The self string is logically split into equal-size segments to generate valid detectors. This produces the collection S of self substrings. In the second step, detectors are randomly generated, and generated strings match strings in S are eliminated. Strings that do not match any string in S are added to the detector set. Two strings match, if they match at least r contiguous locations. Figure 1 shows all these the detector generation phase.

Freitas and Timmis (Freitas and Timmis, 2007) discussed the application of NSA for data mining, so features of NSA were explored. The basic framework of the negative selection process to generate detectors were given in Algorithm 1.

Hofmeyr and Forrest (Hofmeyr and Forrest, 1999),(Hofmeyr and Forrest, 2000) proposed the artificial immune system (ARTIS) method, and they applied it to intrusion detection. This method represents detectors as bit strings, and uses the r contiguous matching rule. Beside these, the study defines the lifecycle of a detector, so it provides dynamic detector populations and adaptation ability in a continuously changing environment. In this lifecycle, a detector can be in one of the five states: immature, mature, activated, memory or death. Figure 2 presents the lifecycle of a detector. Randomly generated detector is considered as immature detectors, and if it does not match

Algorithm 1: Pseudocode of the Negative Selection Process to generate detectors (Freitas and Timmis, 2007).

Data: a set of normal (self) data instances (S)
Result: a set of mature detectors that do not match any instance in S
repeat
  Randomly generate an immature detector
  Measure the affinity (similarity) between this detector and each instance in S)
  if *the affinity between the detector and at least one instance in S is greater than a user-defined threshold* **then**
    discard this detector
  else
    output this detector as a mature immune detector
until *stopping criterion*;

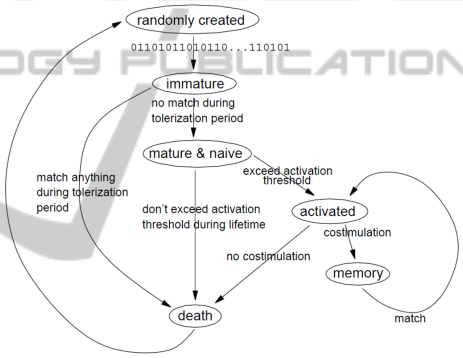

Figure 2: The lifecycle of a detector (Hofmeyr and Forrest, 2000).

self data during the tolerization period, it becomes a mature detector. A mature detector becomes an activated, when it exceeds the activation threshold (match threshold). After that, a human security officer's confirmation (costimulation) is needed for an activated detector to make it a memory detector. Immature, mature and activated detectors can die, but memory detectors go to activated state, when they match non-self. An immature detector dies, if it matches self. A mature detector death is occurred, when it does not exceed activation threshold during lifetime (life expectancy). An activated detector dies, if it does not receive confirmation in a time period (costimulation delay).

Gonzalez et al. (Gonzalez et al., 2003a) presented the effects of the low-level representation and its matching rules on the performance of NSA in covering the non-self space. They explored and compared the different binary matching rules: r-contiguous matching, r-chunk matching, Hamming

distance matching, and Rogers and Tanimoto matching. This study indicates that the matching rule for NSA needs to be chosen when it represents data accurately in problem space.

Gonzalez et al. (Gonzalez et al., 2002) proposed a Real-Valued Negative Selection (RNS) algorithm. RNS algorithm uses real numbers to represent self/non-self space RNS algorithm and binary NSA were compared for anomaly detection problem. Then, advantages and disadvantages of the real-valued representation were presented based on the binary representation. Real-valued representation advantages are: closer to original problem space, allowing the use of methods from computational geometry to speed-up the algorithms, facilitating the use of other machine learning methods to find useful high level knowledge i.e. (Gonzalez and Dasgupta, 2003). Disadvantages of real-valued representation are: making analysis of the problem space harder, not suitable for the representation of categorical attributes.

Dasgupta and Gonzalez (Dasgupta and Gonzalez, 2002) explored positive selection and negative selection, and they were compared using real-valued representation. Detectors are represented as rectangle with real numbers. Based on this comparison, advantages and disadvantages of these approaches were described. This comparison showed that positive selection is more precise, but it needs more time and space resources. The negative selection is less precise, but it needs fewer time and space resources.

Real-valued representation is used in many applications due to the nature of applications' domains, i.e. intrusion detection from network traffic. The non-self coverage gets difficult for the problems with natural real-valued representation. This is because, the real-valued space is continuous and the boundary of self and non-self is ambiguous in this space. Therefore, the non-self coverage is a major issue for real-valued NSA (RNSA) (Gonzalez et al., 2002), (Gonzalez et al., 2003b), (Ji and Dasgupta, 2009), (Zeng et al., 2009), (Balachandran et al., 2007), (X. Yuel and Wangl, 2010). Detector representation and self definition are the determinant for the non-self coverage. A part of research have been focused on the detector representation and distribution in the non-self space in order to maximize the coverage(Gonzalez et al., 2003b), (Balachandran et al., 2007),(Ji and Dasgupta, 2009). On the other hand, the recent research is focused on adaptive-self that implicates the variable self radius (Bezerra et al., 2005), (Zeng et al., 2009), (X. Yuel and Wangl, 2010) . The self radius is an important value to control the detection rate and false alarm rate.

In real-valued NSAs, the detectors are usually represented as circles or rectangles for two dimensional problems. Nevertheless, some NSAs use mixture of specific geometrical shapes to represent the detectors. However, some of NSAs generate the detectors with different sizes. Based on the data and detector representation, the matching rule is changed, and Euclidean distance matching is usually used in real-valued representation.

Dasgupta and Gonzalez (Dasgupta and Gonzalez, 2002), (Gonzalez and Dasgupta, 2002) represent the detectors generated by genetic algorithm as rules. They present the general form of detector rules (detectors) as follows:

$$R_j\text{: If } Cond_i \text{ then nonself, j = 1,...,}x$$

$$Cond_i = x_1 \in [low_1^i, high_1^i] \text{ and ... and } x_n \in [low_n^i, high_n^i]$$

where $(x_1,..., x_n)$ is a feature vector, and $[low_1^i, high_1^i]$ specifies the lower and upper values in the condition part. In this definition, m is the number of detector rules, and n is the number of feature dimensions. The detectors correspond to hyper-rectangles in a multidimensional space. In this study, self region is determined by the level of variability (v) parameter, which is interpreted as the radius of self samples.

Gonzalez et al. (Gonzalez et al., 2003b) proposed a Randomized Real-Valued Negative Selection Algorithm (RRNS). This algorithm takes the detector radius and the self variability threshold (self sample radius) as parameters, so each self sample and detector is represented as circles in two-dimensional problem space. These circles have a fixed size specified by the relevant parameter. Based on the self radius parameter, the algorithm uses Monte Carlo method to estimate the volume of self region.

Balachandran et al (Balachandran et al., 2007) present a work focused on developing a framework for generating multi-shaped detectors in real-valued NSA. This new extended real-valued NSA uses multiple shape (sphere, rectangle or ellipse) detectors for covering two dimensional non-self space. In this NSA, self space is also specified by the constant self radius parameter.

Ji and Dasgupta (Ji and Dasgupta, 2009),(Ji and Dasgupta, 2005),(Ji and Dasgupta, 2004) proposed a new real-valued NSA, which generates variable size detectors. In this NSA, the detectors are represented as circles in two dimensional space and the radii of these circles are variable. On the other hand, the radius for all self samples is taken as the constant parameter and used to check whether a new generated detector is in any self circle or not. If it is, then discarded, otherwise the distance between the center of

detector and the nearest self sample is assigned to this detector radius. This is called boundary-aware method (Ji and Dasgupta, 2005).

In the work by Bezerra et al (Bezerra et al., 2005), an adaptive radius immune algorithm (ARIA) was developed. This is one of the first researches on variable self radius for each self sample. Although, ARIA is closer to clonal selection algorithm, this adjusted self radius has crucial effect in AIS. ARIA considers the density information to form its representation. ARIA takes an initial value of self radius and based on the local density of samples, this initial value is adjusted for each sample.

Zeng et al (Zeng et al., 2009) introduce a self-adaptive negative selection algorithm (ANSA). ANSA can adapt the varieties of self/nonself space by adjusting self radii and detectors' radii. Yuel et al (X. Yuel and Wangl, 2010) worked on optimization of self set for real-valued NSA. In order to do that, self samples are processed in three steps. In the first step, wrong samples are discarded according to "3 σ" criterion. In the next step, the self radius is adjusted by the self's probability density. In the last step, unnecessary self samples, whose covered region is already overlapped by others, are discarded.

The major characteristics of a negative selection algorithm can be identified as follows:

1. Negative representation (Ji and Dasgupta, 2007): NSA identifies and represents the complementary space of the given samples in training phase. Negative representation and positive representation algorithms have been compared in many researches to extract the strength and applicability of negative representation (Dasgupta and Nino, 2000), (Dasgupta and Gonzalez, 2002), (Stibor et al., 2005a), (Stibor et al., 2005b).
2. Usage of detector set as the classification mechanism (Ji and Dasgupta, 2007): Detector set usage provides the opportunity to NSA to distribute its processes, i.e. detectors generation.
3. One-class classification (Ji and Dasgupta, 2007)(Freitas and Timmis, 2007): NSA was developed inspired by the self/non-self discrimination mechanism of the biological mechanism. Therefore, NSA is trained with samples from the one class (self) and then classifies the given instance into one of two classes (self/non-self). Although some researches tried to extend NSA for multiclass classification problems(Dasgupta and Gonzalez, 2002; Gonzalez and Dasgupta, 2002), large majority of the researches have been applied to one-class classification problems.
4. Adaptation capability(Hofmeyr and Forrest, 1999), (Hofmeyr and Forrest, 2000) (Chen et al., 2005): There are many researches to develop adaptive NSAs inspired by the adaptation ability of biological immune system. These adaptive NSAs use some mechanisms, i.e. memory, and processes, to obtain dynamic change of the detectors population.

Particularly, NSA was developed for intrusion detection research (Forrest et al., 1994). Negative selection algorithm (NSA) can be used in many domains today, but the most natural application domain of NSA is intrusion detection (Dasgupta and Gonzalez, 2002), (Powers and He, 2006), (Kim and Bentley, 2001), (Hofmeyr and Forrest, 1999).

2.5 Applications

AIS have many application areas today after first proposal. Hart and Timmis (Hart and Timmis, 2008) surveyed AIS studies and classified application areas of AIS into 12 headings. These categories are presented in table, and according to the number of researches on these categories, categories were divided into major and minor. Based on these categorizations of application areas, Hart and Timmis summarized application areas of AIS as (1) Learning (2) Anomaly Detection and (3) Optimisation. Application areas were mapped to these groups: Learning contains clustering, classification and pattern recognition, robotic and control applications; Anomaly Detection includes fault detection and computer and network security applications; Optimisation consists of real-world problems which essentially include combinatoric and also numeric function optimisation.

Table 1: Application Areas of AIS (Hart and Timmis, 2008).

Major	Minor
Clustering/Classification	Bio-informatics
Anomaly Detection	Image Processing
Computer Security	Control
Numeric Function Optimisation	Robotics
Combinatoric Optimisation	Virus Detection
Learning	Web Mining

Garret (Garrett, 2005) surveyed AIS models and gives the application areas for each of them. NSA application areas are change detection, fault detection and diagnosis, network intrusion detection; Clonal selection application areas are pattern recognition, automated scheduling, document classification, unimodal, combinatorial and multi-modal optimization; Immune network application areas are detecting gene promoter sequences, diagnosis data mining and clus-

ter analysis; Danger theory application area is intrusion detection.

Freitas and Timmis (Freitas and Timmis, 2007) discussed the application of AIS for data mining. They evaluated all AIS models and found limitations in existing AIS for data mining. Limitations they discovered and suggestions for future researches were mentioned in order to mitigate corresponding limitation.

3 CONCLUSIONS

In machine learning, there are many learning methods that are inspired by the biological mechanisms. Genetic algorithm and neural network are the well-known biologically inspired computational models. Genetic algorithm mimics the principles and processes of natural evaluation. On other hand, neural network is inspired by the network or circuit of biological neurons and mimics the properties of biological neurons. Biological immune system is the other biological system that has various computational mechanisms: pattern recognition, memory, distributed processing, self organizing, etc. Inspired by the principles and processes of the biological immune system, many computational intelligent models were developed, and this type of models is called Artificial Immune Systems (AIS). These AIS models are categorized mainly into immune network model, clonal selection, negative selection and danger theory.

REFERENCES

Aickelin, U. and Cayzer, S. (2002). The danger theory and its application to artificial immune systems. In *In Proceedings of the 1st International Conference on Artificial Immune Systems*. Springer-Verlag.

Aickelin, U. and Greensmith, J. (2007). Sensing danger: Innate immunology for intrusion detection. In *Information Security Technical Report*. Elsevier.

Al-Enezi, Abbod, J., and Alsharhan, M. (2010). Artificial immune systems - models, algorithms and application. In *International Journal of Research and Reviews in Applied Sciences*. ARPA Press.

Balachandran, S., Dasgupta, D., Nino, F., and Garrett, D. (2007). A framework for evolving multi-shaped detectors in negative selection. In *In Proceedings of the 2007 IEEE symposium on foundations of computational intelligence*. IEEE Xplore.

Bezerra, G. B., Barra, T. V., de Castro, L. N., and Zuben, F. J. V. (2005). Adaptive radius immune algorithm for data clustering. In *Artificial Immune Systems: 4th International Conference*. Springer-Verlag.

Brownlee, J. (2005). Clonal selection theory and clonalg - the clonal selection classification algorithm (csca). In *Centre for Intelligent Systems and Complex Processes (CISCP), Tech. Rep. 2-02*. Faculty of Information and Communication Technologies (ICT), Swinburne University of Technology.

Chen, J., Liang, F., and Yang, D. (2005). Dynamic negative selection algorithm based on match range model. In *Proceedings of the 18th Australian Joint conference on Advances in Artificial Intelligence*. Springer-Verlag.

Coelho, G. P. and Zuben, F. J. V. (2010). A concentration-based artificial immune network for continuous optimization. In *IEEE Congress on Evolutionary Computation*. IEEE.

Coelho, G. P. and Zuben, F. J. V. (2011). A concentration-based artificial immune network for multi-objective optimization. In *International Conference on Evolutionary Multi-Criterion Optimization*. Springer-Verlag.

Dasgupta, D. and Gonzalez, F. (2002). An immunity-based technique to characterize intrusions in computer networks. In *IEEE Transactions on Evolutionary Computation*. IEEE Press.

Dasgupta, D. and Nino, F. (2000). A comparison of negative and positive selection algorithms in novel pattern detection. In *IEEE International Conference on Systems, Man, and Cybernetics*. IEEE Xplore.

de Castro, L. N. and Zuben, F. J. V. (1999). Artificial immune systems: part i - basic theory and applications. In *Technical Report DCA-RT 01/99*. School of Computing and Electrical Engineering, State University of Campinas.

de Castro, L. N. and Zuben, F. J. V. (2000). The clonal selection algorithm with engineering applications. In *Proceedings of the Genetic and Evolutionary Computation Conference*. Morgan Kaufmann.

de Castro, L. N. and Zuben, F. J. V. (2001). ainet: An artificial immune network for data analysis. In *In Data Mining: A Heuristic Approach*. Idea Group.

de Castro, L. N. and Zuben, F. J. V. (2002). Learning and optimization using the clonal selection principle. In *IEEE Transactions on Evolutionary Computation*. IEEE Press.

Forrest, S., Perelson, A., Allen, L., and Cherukuri, R. (1994). Self-nonself discrimination in a computer. In *In Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy*. IEEE Computer Society.

Freitas, A. A. and Timmis, J. (2007). Revisiting the foundations of artificial immune systems for data mining. In *IEEE Transactions on Evolutionary Computation*. IEEE Press.

Garrett, S. M. (2005). How do we evaluate artificial immune systems? In *Evolutionary Computation*. MIT Press.

Gonzalez, F. and Dasgupta, D. (2002). An immunogenetic technique to detect anomalies in network traffic. In *In Proceedings of the genetic and evolutionary compuation conference*. Morgan Kaufmann.

Gonzalez, F. and Dasgupta, D. (2003). Anomaly detection using real-valued negative selection. In *Genetic Programming and Evolvable Machines*. Kluwer Academic.

Gonzalez, F., Dasgupta, D., and Gomez, J. (2003a). The effect of binary matching rules in negative selection. In *In Proceedings of the Genetic and Evolutionary Computation Conference (GECCO 2003)*. Springer-Verlag.

Gonzalez, F., Dasgupta, D., and Kozma, R. (2002). Combining negative selection and classification techniques for anomaly detection. In *Proceedings of the 2002 Congress on Evolutionary Computation*. IEEE Computer Society.

Gonzalez, F., Dasgupta, D., and Nino, L. F. (2003b). A randomized real-valued negative selection algorithm. In *In Proceedings of the 2nd International Conference on Artificial Immune Systems*. Springer-Verlag.

Greensmith, J., Aickelin, U., and Twycross, J. (2004). Detecting danger: Applying a novel immunological concept to intrusion detection systems. In *Proceedings of the 6th International Conference in Adaptive Computing in Design and Manufacture*. Springer-Verlag.

Hart, E. and Timmis, J. (2008). Application areas of ais: The past, the present and the future. In *Applied Soft Computing*. Elsevier Science.

Hofmeyr, S. A. and Forrest, S. (1999). Immunity by design: An artificial immune system. In *In Proceedings of the Genetic and Evolutionary Computation Conference*. Morgan Kaufmann.

Hofmeyr, S. A. and Forrest, S. (2000). Architecture for an artificial immune system. In *Evolutionary Computation Journal*. MIT Press.

Jerne, N. (1974). Towards a network theory of the immune system. In *Annals of Immunology*. Inst. Pasteur.

Ji, Z. and Dasgupta, D. (2004). Real-valued negative selection algorithm with variable-sized detectors. In *In proceeding of Genetic and Evolutionary Computation*. Springer-Verlag.

Ji, Z. and Dasgupta, D. (2005). A boundary-aware negative selection algorithm. In *In Proceedings of the international conference on artificial intelligence and soft computing*. ACRA Press.

Ji, Z. and Dasgupta, D. (2007). Revisiting negative selection algorithms. In *MIT Evolutionary Computation*. MIT Press.

Ji, Z. and Dasgupta, D. (2009). V-detector: An efficient negative selection algorithm with 'probably adequate' detector coverage. In *Information Sciences*. Elsevier Science.

Kim, J. and Bentley, P. J. (2001). An evaluation of negative selection in an artificial immune system for network intrusion detection. In *Proceedings of the Genetic and Evolutionary Computation Conference*. Morgan Kaufmann.

Kim, J., Greensmith, J., Twycross, J., and Aickelin, U. (2005). Malicious code execution detection and response immune system inpired by the danger theory. In *Proceedings of the Adaptive and Resilient Computing Security Workshop (ARCS-05)*.

L. O. V. B. Oliveira, R. L. M. Motay, D. A. C. B. (2012). Clonal selection classifier with data reduction: Classification as an optimization task. In *IEEE World Congress on Computational Intelligence*. IEEE.

Li, J., Gao, H., and Wang, S. (2012). A novel clone selection algorithm with reconfigurable search space ability and its application. In *Fourth International Conference on Natural Computation*. IEEE Computer Society.

Liu, L. and Xu, W. (2008). A cooperative artificial immune network with particle swarm behavior for multimodal function optimization. In *IEEE Congress on Evolutionary Computation*. IEEE Press.

Matzinger, P. (2002). The danger model: A renewed sense of self. In *Science*.

Powers, S. T. and He, J. (2006). Evolving discrete-valued anomaly detectors for a network intrusion detection system using negative selection. In *In the 6th Annual Workshop on Computational Intelligence (UKCI '06)*. University of Leeds.

Roper, M. (2009). Artifical immune systems, danger theory, and the oracle problem. In *Testing: Academic and Industrial Conference - Practice and Research Techniques*. IEEE Computer Society.

Stibor, T., Mohr, P., Timmis, J., and Eckert, C. (2005a). Is negative selection appropriate for anomaly detection? In *Proceedings of the 2005 conference on Genetic and evolutionary computation*. ACM.

Stibor, T., Timmis, J., and Eckert, C. (2005b). A comparative study of real-valued negative selection to statistical anomaly detection techniques. In *Proceedings of the 4th international conference on Artificial Immune Systems*. Springer-Verlag.

Timmis, J. and Neal, M. (2001). A resource limited artificial immune system for data analysis. In *Knowledge Based Systems*. Elsevier.

Timmis, J., Neal, M., and Hunt, J. (2000). An artificial immune system for data analysis. In *Biosystems*. Elsevier.

X. Yuel, F. Zhang, L. X. and Wangl, D. (2010). Optimization of self set and detector generation base on real-value negative selection algorithm. In *2010 International Conference on Computer and Communication Technologies in Agriculture Engineering*. IEEE Xplore.

Zeng, J., Liu, X., Li, T., Liu, C., Peng, L., and Sun, F. (2009). A self-adaptive negative selection algorithm used for anomaly detection. In *Progress in Natural Science*. Elsevier.

Zhong, Y. and Zhang, L. (2012). An adaptive artificial immune network for supervised classification of multi-/hyperspectral remote sensing imagery. In *IEEE Transactions on Geoscience and Remote Sensing*. IEEE.

Zhu, Y. and Tan, Y. (2011). A danger theory inspired learning model and its application to spam detection. In *Proceedings of the second international conference on advances in swarm intelligence*. Springer-Verlag.