Further Developments on Router Nodes Positioning for Wireless Networks using Artificial Immune Systems

Pedro Henrique Gouvêa Coelho, J. L. M. do Amaral, J. F. M. do Amaral, L. F. de A. Barreira and A. V. de Barros
State Univ. of Rio de Janeiro, FEN/DETEL, R. S. Francisco Xavier, 524/Sala 5001E, Maracanã, RJ, 20550-900, Brazil

Keywords: Artificial Immune Systems, Artificial Intelligence Applications, Node Positioning, Wireless Networks.

Abstract: This paper shows further developments on the positioning of intermediate router nodes using artificial immune systems for use in industrial wireless sensor networks. These nodes are responsible for the transmission of data from sensors to the gateway in order to meet criteria, especially those that lead to a low degree of failure and reducing the number of retransmissions by routers. In the present paper positioning configurations on environments in presence of obstacles is included. Affinity functions which roles are similar to optimization functions are explained in details and case studies are included to illustrate the procedure. As was done in previous papers, positioning is performed in two stages, the first uses elements of two types of immune networks, SSAIS (Self-Stabilising Artificial Immune System) and AINET (Artificial Immune Network), and the second uses potential fields for positioning the routers such that the critical sensors attract them while obstacles and other routers repel them.

1 INTRODUCTION

Wireless industrial sensor network is an emerging field including a great deal of research work involving hardware and system design, networking, security factor and distributed algorithms (Coelho et al., 2013), (Coelho et al., 2014), (Dai and Li, 2005), (Akyildiz et al., 2002). Sensor nodes usually sense the data packet and transfer it to the gateway via some intermediate nodes. The sensor nodes consist of low cost, low power and short transmission range (Coelho et al., 2014). Main advantages are reduced installation time of devices, no need of cabling structure, cost saving projects, infrastructure savings, device configuration flexibility, cost savings in installation, flexibility in changing the existing architectures, possibility of installing sensors in hard-to-access locations and others. Safety, reliability, availability, robustness and performance are key issues in the area of industrial automation. Data transmission in a wireless network may suffer the problem of interference generated by other electrical networks and electrical equipment, moving obstacles (trucks, cranes, etc.) and fixed ones (buildings, pipelines, tanks, etc.). In an attempt to minimize these effects, frequency scattering techniques and mesh or tree topologies are used, in which a message can be transmitted from one node to another with the aid of other nodes, which act as intermediate routers, directing messages to other nodes until it reaches its final destination. This allows the network to get a longer range and to be nearly fault tolerant, because if an intermediate node fails or cannot receive a message, that message could be routed to another node. However, a mesh network also requires careful placement of these intermediate nodes, since they are responsible for doing the forwarding of the data generated by the sensor nodes in the network to the gateway directly or indirectly, through hops. Those intermediate nodes are responsible for meeting the criteria of safety, reliability and robustness of the network and are also of paramount importance in the forwarding of data transmission. They could leave part or all the network dead, if they display any fault (Hoffert et al., 2007). Most solutions to the routers placement solve this problem with optimization algorithms that minimize the number of intermediate router nodes to meet the criteria for coverage, network connectivity and longevity of the network and data fidelity. (Youssef and Younis, 2007), (Molina et al., 2008). Recently, (Lanza-Gutiérrez and Pulido, 2016) considered router nodes deployment in wireless sensor networks with the purpose of optimizing the

Coelho, P., Amaral, J., Amaral, J., Barreira, L. and Barros, A.
Further Developments on Router Nodes Positioning for Wireless Networks using Artificial Immune Systems.
In *Proceedings of the 18th International Conference on Enterprise Information Systems (ICEIS 2016) - Volume 2*, pages 99-105
ISBN: 978-989-758-187-8

average energy consumption of the sensors and average sensitivity area provided by the network. This paper considers further developments to a previous paper by the authors (Coelho et al., 2014) which used Artificial Immune Networks for node positioning. The algorithms based on immune networks have very desirable characteristics in the solution of this problem, among which we can mention: scalability, self-organization, learning ability and continuous treatment of noisy data (Coelho et al., 2013). The improvements done included modifications in the affinity function to consider obstacles and case studies for different configurations. This paper is divided into four sections. Section 2 does a brief discussion of artificial immune systems. Section 3 presents the application of artificial immune systems to the problem of node positioning where the affinity function is discussed in details. Section 4 ends the paper by presenting results and conclusions.

2 IMMUNE SYSTEM BASICS

The immune system is a biological mechanism for identifying and destroying pathogens within a larger organism (Amaral, 2006). Pathogens are agents that cause disease such as bacteria, viruses, fungi, worms, etc. Anything that causes an immune response is known as an antigen. An antigen may be harmless, such as grass pollen, or harmful, such as the flu virus. In other words disease-causing antigens are called pathogens. So the immune system is designed to protect the body from pathogens. In humans, the immune system begins to develop in the embryo. The immune system begins with hematopoietic, (i.e. blood-making from Greek) stem cells. These stem cells differentiate into the major players in the immune system e.g. granulocytes, monocytes, and lymphocytes. These stems cells also differentiate into cells in the blood that are not connected to immune function, such as erythrocytes e.g. red blood cells, and megakaryocytes for blood clotting. Stem cells continue to be produced and differentiate throughout our lifetime. The immune system is usually divided into two categories--innate and adaptive--although these distinctions are not mutually exclusive. The innate subsystem is similar in all individuals of the same species, whereas the adaptive subsystem depends on the experience of each individual i.e. exposure to infectious agents. The innate immune response is able to prevent and control many infections. Nevertheless, many pathogenic microbes have evolved to overcome innate immune defenses, and so to protect ourselves against these infections, we have to call in the more powerful mechanisms of adaptive immunity. Adaptive immunity is normally silent, and responds or adapts to the presence of infectious microbes by becoming active, expanding, and generating potent mechanisms for neutralizing and eliminating the microbes. The components of the adaptive immune subsystem are lymphocytes and their products. The most notable cells of adaptive immunity are lymphocytes. There are two main classes of lymphocytes. B lymphocytes, named so, because they mature in the bone marrow, secrete proteins called antibodies, which bind to and eliminate extracellular microbes. T lymphocytes, which mature in the thymus, and function mainly to combat microbes that have learned to live inside cells where they are inaccessible to antibodies. The normal immune system has to be capable of recognizing virtually any microbe and foreign substance that one might encounter, and the response to each microbe has to be directed against that microbe. The substances that are recognized by these lymphocytes are called antigens. The immune system recognizes and directs responses against a massive number of antigens by generating a large number of lymphocytes, each with a single antigen receptor. Therefore, there are about 10^{12} lymphocytes in an adult, and it is estimated that these are able to recognize at least 10^7 – 10^9 different antigens (Silva, 2001). Thus, only a few thousand lymphocytes express identical antigen receptors and recognize the same antigen. The antigen receptors of B cells are membrane-bound antibodies, also called immunoglobulins, or Ig. Antibodies are Y-shaped structures (Jerne, 1974). The tops of the Y recognize the antigen and, in B cells, the tail of the Y anchors the molecule in the plasma membrane. Antibodies are capable of recognizing whole microbes and macromolecules as well as small chemicals. These could be in the circulation e.g. a bacterial toxin, or attached to cells (e.g. a microbial cell wall component. The antigen receptors of T cells are structurally similar to antibodies, but T cell receptors (TCRs) recognize only small peptides that are displayed on specialized peptide-display molecules (Castro and Von Zuben, 1999). Although the immune system is capable of recognizing millions of foreign antigens, it usually does not react against one’s own, i.e. self, antigenic substances. This is because lymphocytes that happen to express receptors for self-antigens are killed or shut off when they recognize these antigens. This phenomenon is called self-tolerance, implying that we tolerate our own antigens and the breakdown of this process yields in autoimmune diseases. When one antibody binds to other material, the lymphocyte carrying it, is stimulated to reproduce by cloning, this is known as Clonal selection principle. Genes coding lymphocytes have a mutation rate above normal, one mutation per cell division, on average, leading to what is known as somatic hypermutation. Clonal selection and hypermutation increases affinity between antibodies and antigens. There are three steps for an Artificial Immune System (AIS). First, find a representation of the components i.e. artificial equivalents to cells and antigens. Second, define affinity functions between components in order to quantify interaction among them. Third, write a set of immune algorithms that control system behavior. Why would a computer scientist get the trouble to study immune systems? Immune systems are massively parallel information processing mechanisms and are incredibly effective examples of distributed systems built from diverse components which are constantly being renewed. So that may inspire better computer security systems, for example, because of their adaptiveness, they can train themselves to react to new threats. Moreover they are error—tolerant, so that small mistakes are not fatal, and also self-protecting.

3 ROUTER NODE POSITIONING USING ARTIFICIAL IMMUNE SYSTEMS

Node positioning based on artificial immune networks presented in this paper aims to establish two or more disjoint paths from the sensor nodes to the gateway by removing, cloning and reconfiguring intermediate router nodes. In addition, the method is also able to meet the criteria of low fault degree and low number of relay routers. These criteria can be enabled individually or combined with equal or different weights at user's discretion. The positioning algorithm is made on two modules: (i) Immune Network - combines elements of two models of immune networks: Self-Stabilizing Artificial Immune System - SSAIS (Neal, 2002) and Artificial Immune Network - Ainet (Castro and Von Zuben, 1999); (ii) Potential Fields - positions router nodes by potential fields where the critical sensors attract them while obstacles and other routers repel them. The use of wireless sensor network in industrial automation is still a matter of concern with respect to the data reliability and security by users. Thus, an appropriate node positioning is of paramount importance for the wireless network to meet safety, reliability and efficiency criteria. Positioning of nodes is a difficult task, because one should take into account all the obstacles and interference present in an industrial environment. The gateway as well as the sensors generally have a fixed position near the control room. But the placement of router nodes, which are responsible for routing the data, generated by the sensors network to the gateway directly or indirectly, is determined by the characteristics of the network. The main characteristics of wireless sensor networks for industrial automation differ from traditional ones by the following aspects: The maximum number of sensors in a traditional wireless network is on the order of millions while automation wireless networks is on the order of tens to hundreds; The network reliability and latency are essential and fundamental factors for network wireless automation. To determine the number of router nodes and define the position in the network, some important aspects in industrial automation should be considered. It should be guaranteed: (1) redundant paths so that the system be node fault-tolerant; (2) full connectivity between nodes, both sensors and routers, so that each node of the network can be connected to all the others exploring the collaborative role of routers; (3) node energy efficiency such that no node is overwhelmed with many relaying information from the sensors; (4) low-latency system for better efficiency in response time; (5) combined attributes for industrial processes to avoid accidents due to, for example, high monitored process temperature. (6) self-organization ability, i.e. the ability of the network to reorganize the retransmission of data paths when a new sensor is added to the network or when a sensor stops working due to lack of power or a problem in wireless communication channel. All these factors must be met, always taking into consideration the prime factor security: the fault tolerance. In the end of the router nodes placement, the network of wireless sensors applied to industrial automation should be robust, reliable, scalable and self-organizing.

The positioning of router nodes in industrial wireless sensor networks is a complex and critical task to the network operation. It is through the final position of routers that one can determine how reliable, safe, affordable and robust the network is. In the application of immune systems to router nodes positioning reported in this paper, B cells that make up the immune network will be composed by a set of sensor nodes and a set of router nodes. The sensor nodes are located in places where the plant instrumentation is required. These nodes have fixed coordinates, i.e. they cannot be moved. For security to be guaranteed it is necessary to have redundant paths between these nodes and the gateway. The set of router nodes will be added to allow redundant paths. The position of these nodes will be changed during the process of obtaining the final network. After the inclusion of the new router nodes, a stop condition is performed. If the condition is not met, all routers undergo an action of repulsive forces, generated by obstacles and routers for other nodes, followed by attractive forces created by critical sensor nodes. Those critical nodes are the ones that do not meet the minimum number of paths necessary to reach the gateway. The actions of repelling potential fields have the function of driving them away from obstacles, to allow direct line of sight for the router network nodes to increase the reliability of transmission and also increase the distance among the routers to increase network coverage. On the other hand, the attractive potential fields attract routers to critical sensors, easing the formation of redundant paths among sensors and the gateway. After the action of potential fields, from the new positioning of routers, a new network is established and the procedure continues until the stopping criterion is met. The algorithm proposed in this paper deals with a procedure based on artificial immune networks, which solves the problem of positioning the router nodes so that every sensor device is able to communicate with the gateway directly and or indirectly by redundant paths. Figure 1 shows the main modules of the algorithm. The first module is called immune network, and the second, positioning module is called potential fields containing elements used in positioning sensor networks using potential fields (Howard, 2002). The immune network module performs an algorithm that can be described by the following steps:

Creation: Creation of an initial set of cells to form a network.

Evaluation: Determination of the cells affinity to calculate their stimulation.

Pruning: Performs the resource management and remove cells that are without resources from the network.

Selection: Selects the more stimulated cells to be cloned.

Cloning: Generates a set of clones from the most stimulated cells.

Mutation: Does the mutation of cloned cells.

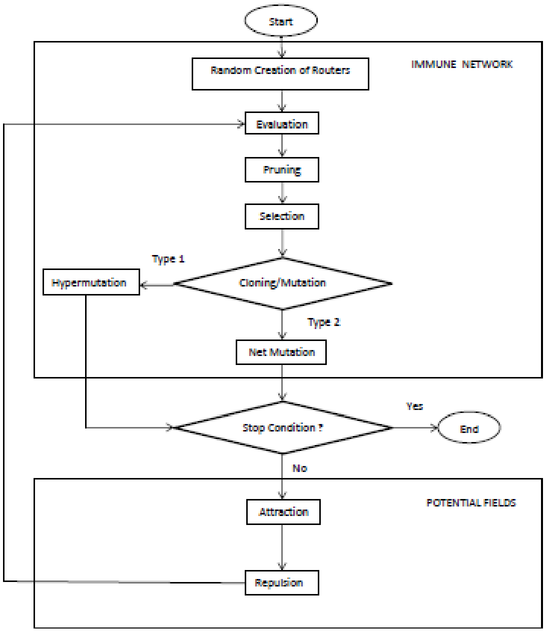

Figure 1: The AIS based algorithm.

In the stage of creation, an initial set of routers is randomly generated to initiate the process of obtaining the network, and the user can specify how many routers to place it initially. In the evaluation phase, a network which is represented by a graph is formed with sensor nodes and router nodes. From this graph, values of several variables are obtained that will be used to calculate the affinity. Examples of such variables are the number of paths that exist between each sensor and the gateway, the number of times that a router is used on the formed paths, etc. The affinity (Af) is given by equation 1 and consists of a weighted sum of the three affinities that are enabled at the discretion and need of the users. Thus, if a user believes that affinity1 and affinity3, for example, are critical to his network, he may disable the other affinities and choose the weights so that the sum is 1 for the enabled parts.

$$Af = w1*Afinity1 + w2*Afinity2 + w3*Afinity3 \qquad (1)$$

Afinity1 takes into account the failure degree of each router. It is given by the normalized difference between the total number of paths between the sensors and the gateway and the number of remaining paths when the examined router is taken out. In other words the higher the degree of failure, the greater the affinity1 and therefore more critical will be loss of the examined router for the network.

Affinity2 sets the number of times the router is used as a function of the path. It is calculated by the ratio of the number of times that the router is used in the observed paths and the number of paths that should exist, according to user specification. The more the router is used, the greater the affinity2.

Finally, affinity3 is related to the neighbouring sensors for the examined node. Affinity3 lies between 0 and 1, where 1 is the critical value for the network.

4 RESULTS AND CONCLUSIONS

Case studies were simulated in a 1 x 1 square scenario. The cloning procedure considered that only the router with higher affinity would be selected to produce three clones in each generation. For each case study 10 experiments were conducted that demonstrate the algorithm's ability to create at least two redundant paths to get the information from any sensor to the gateway. Two configurations were considered to demonstrate the proposed router nodes positioning algorithm in environments with obstacles. The configurations used in the simulation were motivated by oil & gas refinery automation applications. The first configuration (PosA) comprises two circular obstacles with a radius of 0.1, and five nodes, in which node 1 is the gateway and the others are sensor nodes.

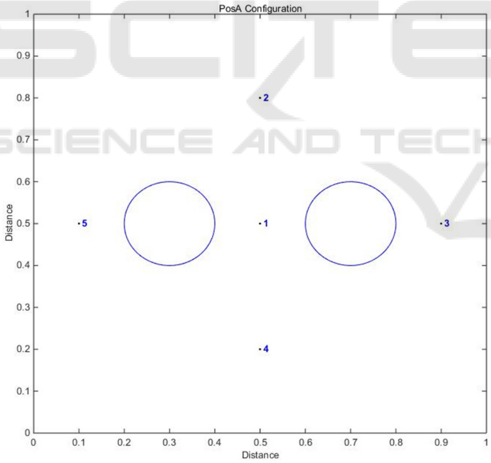

Figure 2: Sensors and gateway POSA configuration. (Legend: node 1:gateway; nodes 2 to 5: sensors).

Initially, the gateway has not direct line of sight with sensor nodes 3 and 5 and is not connected, i.e. out of range, to any of the network nodes, as depicted in Figure 2.

The second configuration (PosB) has eight obstacles: three circular ones have radius of 0.05, another circular one has radius 0.15 and four rectangular obstacles with different sizes.

Besides, the gateway is node 1 and nodes 2 to 8 are the seven sensor *nodes.* The second configuration (PosB) has eight obstacles: three circular ones have radius of 0.05, another circular one has radius 0.15 and four rectangular obstacles with different sizes. Besides, the gateway is node 1 and nodes 2 to 8 are the seven sensor nodes. Initially, the gateway has not direct line of sight to any of the sensor nodes and is not connected to any network node as it is out range to the other nodes. Moreover, sensor nodes do not have a direct line of sight with each other and are not connected as they are out of range with each other too. Figure 3 shows the PosB configuration. In this section, case studies 1 and 2 are considered for configurations PosA and PosB. For case study 1, the network configuration is cross-shaped, the operating range of the network nodes is 0.2 and the positioning procedure led to two disjoint paths for the sensors send data to the gateway. Case study 2 uses configuration PosB and considers the same operating range as in the case study 1, 0.2, and now three disjoint paths are required.

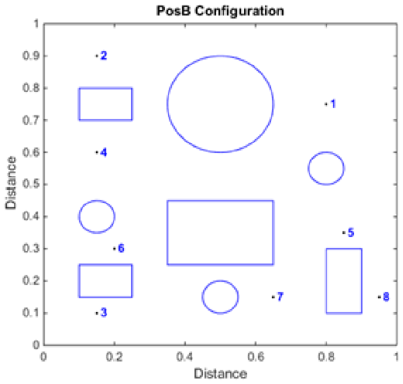

Figure 3: Sensors and gateway POSB configuration. (Legend: node 1:gateway; nodes 2 to 8 :sensors).

Tables 1 and 3 show the used parameters for case studies 1 and 2. Figure 4 shows the best configuration obtained from the 10 experiments. Table 2 shows the network performance for case study 1.

Table 1: Case study 1 – POSA configuration parameters.

Simulation Parameters	Values	Method
Number of generations	30	-
Initial number of Routers	10	-
Affinity	-	Failure Degree, Number of Times A router is used and Number of neighbour sensors

Table 2: Network performance for case study 1.

Network	Min.	Av.	Max.	St. Dev.
No. of nodes	19	19.9	22	0.99
No. of routers	14	14.9	17	0.99
No. of critical sensors	0	0	0	-
No. a router is used	2	2	2	0

It can be seen in Figure 4 that the sensor nodes 3 and 5 in the paths 3-16-17-20-1, 3-19-7-10-1, 5-13-11-18-1 and 5-12-14-15-1 show four jumps to the gateway. This means the data sent by these devices suffer a delay when received by the gateway, since it will need to be relayed through three intermediate nodes.

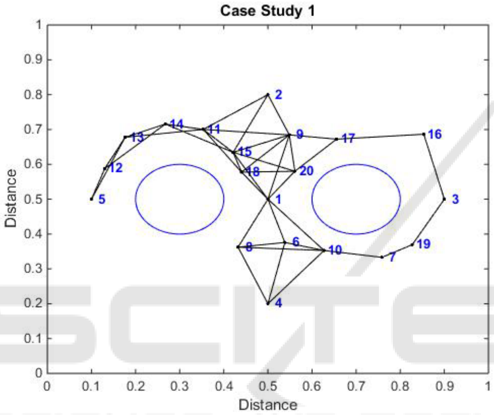

Figure 4: Node positioning for case study 1 in POSA configuration.

Table 3: Case study 2 – POSB configuration parameters.

Simulation Parameters	Values	Method
Number of generations	100	-
Initial number of Routers	10	-
Affinity	-	Failure Degree, No. of times a router is used and No. of neighbour sensors

Table 4: Network performance for case study 2.

Network	Min.	Av.	Max.	St. Dev.
No. of nodes	59	60.5	63	1.18
No. of routers	51	52.5	55	1.18
No. of critical sensors	0	0	0	-
No. a router is used	5	5.4	8	0.97

With respect to the failure degree, the intermediate nodes 7, 10, 11, 12, 13, 14, 16, 17 and 19 have a 30% failure degree, and the other router nodes have an index lower than 30%. So 70% of the paths from the sensors to the gateway, continue to exist even after the removal of a node. Figure 5 shows the best configuration out of ten experiments for case study 2 and table 4 shows the network performance for case study 2. Figure 4 indicates that for sensor nodes 3 and 6, the paths 3-20-22-24-7-40-63-53-36-1, 3-50-49-61-4-52-15-56-39-1 and 6-58-61-4-60-31-15-37-26-1 show nine hops to the gateway. This means that the data sent by these devices suffer a delay in the gateway, since it will need to be relayed by eight intermediate nodes. With respect to the failure degree, the router node 32 have 21% failure degree, and the other router nodes have an index lower than 21%. This means that 79% of the paths from the sensors are still present even after a node removal.

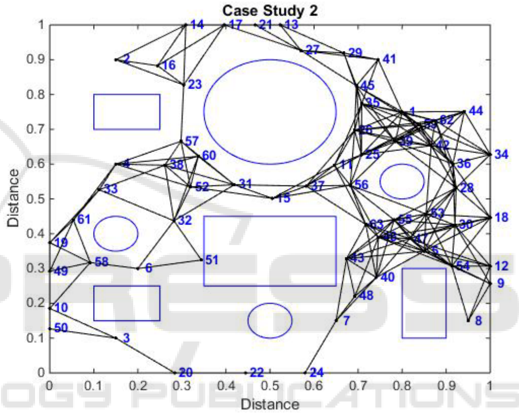

Figure 5: Node positioning for case study 1 in POSB configuration.

This work proposed a positioning algorithm for router nodes in wireless network using immune systems techniques. The algorithm creates redundant paths to the data collected by the sensors to be sent to the gateway by any two or more paths, meeting the criteria of degree of failure, the number of retransmission by routers and number of sensors to neighbouring routers. The algorithm allows each criterion is enabled at a time or that they be combined with weights. The affinity function, which works as an objective function, is multi-objective, so several other objectives could be jointly considered. Future work will try to consider a comparison of this work among the several related works existing in the literature taking into account the different scenarios and the objectives of each approach. A suitable benchmark problem would be important for the comparisons. Due to the distinct objectives assumed in each work the comparison task will not be an easy one.

REFERENCES

Dai S., Jing X., and. Li L, 2005. Research and analysis on routing protocols for wireless sensor networks. *In Proc. International Conference on Communications, Circuits and Systems*, Volume 1, pp. 407-411.

Akyildiz F., Su W., Sankarasubramaniam, Y. and Cayirci, E., 2002. Wireless Sensor Networks: A Survey, Computer Networks, 38, pp. 393-422.

Coelho, P. H. G., Amaral, J. L. M., Amaral, J. F. M., Barreira, L.F.A. and, Barros, A. V., 2013. Deploying Nodes for Industrial Wireless Networks by Artificial Immune Systems Techniques. In *15th International Conference on Enterprise Information Systems*, Angers, France.

Coelho, P. H. G., Amaral, J. L. M., Amaral, J. F. M., Barreira, L.F.A. and, Barros, A. V., 2014. Router Nodes Positioning for Wireless Networks Using Artificial Immune Systems. In *16th International Conference on Enterprise Information Systems*, Lisbon, Portugal.

Hoffert, J., Klues, K., and Orjih, O., 2007. *Configuring the IEEE 802.15.4 MAC Layer for Single-sink Wireless Sensor Network Applications,* Technical Report http://www.dre.vanderbilt.edu/~jhoffert/802_15_4_Eval_Report.pdf.

Youssef, W., and Younis, M., 2007. Intelligent Gateways Placement for Reduced Data Latency in Wireless Sensor Networks. In *ICC'07 International Conference on Communications, Glasgow,* pp.3805-3810.

Molina, G., Alba, E., and Talbi, E. G., 2008. Optimal Sensor Network Layout Using MultiObjective Metaheuristics. *Journal of Universal Computer Science,* Vol.15, No. 15, pp.2549-2565.

Lanza-Gutiérrez, J. M., and Pulido, J. A. G., 2016. Studying the multiobjective variable neighbourhood search algorithm when solving the relay node placement problem in Wireless Sensor Networks. *Soft Computing* , Vol. 20 pp. 67-86.

Silva, L. N. C., 2001. *Immune Engineering: Development and Application of Computational Tools Inspired by Artificial Immune Systems*, Ph. D. Thesis, State University of Campinas, Campinas, in portuguese.

Amaral, J. L. M., 2006. *Artificial Immune Systems Applied to Fault Detection*, Ph. D. Thesis, Pontifical Catholic University of Rio de Janeiro, Rio de Janeiro, in portuguese.

Jerne, N. K., 1974. Towards a Network Theory of the Immune System. *Ann. Immunol. (Inst. Pasteur),* 125C, pp. 373-389.

Howard, A., Mataric, M. J., and Sukhatme, G. S., 2002. Mobile Sensor Network Deployment using Potential Fields: A Distributed, Scalable Solution to the Area Coverage Problem heuristics. In *DARS'02, 6th International Symposium on Distributed Autonomous Robotics Systems,* Fukuoka, Japan.

Howard, A., Mataric, M. J., Sukhatme, G. S., 2002. Mobile Sensor Network Deployment using Potential Fields: A Distributed, Scalable Solution to the Area Coverage Problem. *Proceedings of the 6th International Symposium on Distributed Autonomous Robotics Systems (DARS02)*, Fukuoka, Japan, pp. 299-308.

Timmis, J., and Neal, M. , 2001. A Resource Limited Artificial Immune System for Data Analysis. *Knowledge Based Systems,* Vol.3-4, No. 14, pp.121-130.

Neal, M., 2002. An Artificial Immune System for Continuous Analysis of Time-Varying Data. In *1st ICARIS.*

Castro, L. N., Von Zuben, F. J., 1999. Artificial Immune Systems: Part I – Basic Theory and Applications. Technical Report TR-DCA 01/99.