Router Nodes Positioning for Wireless Networks Using Artificial Immune Systems

P. H. G. 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 proposes 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. These criteria can be enabled individually or in groups, combined with weights. 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. Case studies are presented to illustrate the procedure.

1 INTRODUCTION

Data transmission through the use of wireless technology has grown dramatically in society. The wireless technology has taken over the world and the field of industrial automation is no exception. 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 of paramount importance in the area of industrial automation. The network cannot be sensitive to interference nor stop operation because of an equipment failure, nor can have high latency in data transmission and ensure that information is not misplaced (Zheng and Lee, 2006). In industrial automation environment, data transmission in a wireless network faces the problem of interference generated by other electrical equipment, such as walkie-talkies, other wireless communication 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). This paper proposes to solve this problem using Artificial Immune Networks, based on the human immune system. 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., 2012). This paper is divided into four

H. G. Coelho P., L. M. do Amaral J., F. M. do Amaral J., F. de A. Barreira L. and V. de Barros A..
Router Nodes Positioning for Wireless Networks Using Artificial Immune Systems.
DOI: 10.5220/0004898904150421
In *Proceedings of the 16th International Conference on Enterprise Information Systems* (ICEIS-2014), pages 415-421
ISBN: 978-989-758-027-7

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 and section 4 concludes the paper by presenting results and conclusions.

2 IMMUNE SYSTEMS

Artificial immune systems (AISs) are models based on natural immune systems which protect the human body from a large number of pathogens or antigens (Amaral, 2006). Due to these characteristics the AISs are potentially suitable for solving problems related to computer security and they inherit from natural immune systems the properties of uniqueness, distributed sensing, learning and memory efficiency. In fact, the immune system is unique to each individual. The detectors used by the immune system are small, efficient and highly distributed and are not subject to centralized control. Moreover, it is not necessary that every pathogen is fully detected, because the immune system is more flexible, there is a compromise between the resources used in the protection and breadth in coverage. Anomaly detection is another important feature, since it allows the immune system to detect and respond to pathogens (agents that cause diseases) for which they have not previously been found. The immune system is able to learn the structures of pathogens and remember these structures so that future responses to these agents are faster. In summary, these features make the immune system scalable, robust and flexible. The immune system uses distributed detection to distinguish the elements of the organism itself, the self, and foreign to the body, the non-self. The detection of the non-self is a difficult task because its number, of the order of 10^{16}, is much superior to the number of self patterns, around 10^{6}, taking place in a highly distributed environment. It should be also noted that all these actions occur while the living organism must continue in operation and the available resources are scarce. Cells that perform the detection or recognition of pathogens in the acquired or adaptive immune system are called lymphocytes that recognize pathogens joining them. The antigens are detected when a molecular bond is established between the pathogens and the receptors present on the surface of lymphocytes. A given receiver will not be able to join all antigens. A lymphocyte has approximately 100,000 receptors on its surface which however have the same structure, and therefore can only join with structurally related epitopes (the site on an antigen at which a specific antibody becomes attached). Such epitopes define a similarity subset of epitopes which lymphocytes can detect. The number of receivers that can join the pathogens defines the affinity of a lymphocyte to a certain antigen. Lymphocytes can only be activated by an antigen if their affinities exceed a certain threshold. As this threshold increases, the number of epitopes types capable of activating a lymphocyte decreases, i.e., the similarity subset becomes smaller. A receiver may be obtained by randomly recombining possible elements (from the memory of the immune system), producing a large number of possible combinations indicating a wide range in the structure of the receptors. Although it is possible to generate approximately 10^{15} receptor types, the number present at a given instant of time is much smaller, in the range of 10^{8} to 10^{12} (Silva, 2001). The detection is approximate, since it is a difficult task to evolve structures that are complementary to receptor epitopes for which the organism has never encountered before. If an exact complementarity was needed, the chance of a random lymphocyte epitope join a random would be very small. An important consequence of that approximate detection is that one single lymphocyte is capable of detecting a subset of epitopes, which implies that a smaller number of lymphocytes is required for protection against a wide variety of possible antigens. The main algorithms that implement the artificial immune systems were developed from metaphors of the immune system: the mechanism of negative selection, the theory of immune network and the clonal selection principle. The function of the negative selection mechanism is to provide tolerance to the self cells, namely those belonging to the organism. Thus, the immune system gains the ability to detect unknown antigens and not react to the body's own cells. During the generation of T-cells, which are cells produced in the bone marrow, receptors are generated by a pseudo-random process of genetic arrangement. Later on, they undergo a maturation mechanism in the thymus, called negative selection, in which T cells that react to body proteins are destroyed. Thus, only cells that do not connect to the body proteins can leave the thymus. The T cells, known as mature cells, circulate in the body for immune functions and to protect it against antigens. The theory of immune system network considers several important aspects like the combination of antibodies with the antigens for the early elimination of the antigens. Each antibody has its own antigenic determinant, called

idiotope. In this context, (Jerne, 1974) proposed the Immune Network Theory to describe the activity of lymphocytes in an alternative way. According to (Jerne, 1974) the antibodies and lymphocytes do not act alone, but the immune system keeps a network of B cells for antigen recognition. These cells can stimulate and inhibit each other in various ways, leading to stabilization of the network. Two B cells are connected if they share an affinity above a certain threshold and the strength of this connection is directly proportional to the affinity they share. The clonal selection principle describes the basic features of an immune response to an antigenic stimulus, and ensures that only cells that recognize the antigen are selected to proliferate. The daughter cells are copies or clones of their parents and are subject to a process of mutation with high rates, called somatic hypermutation. In the clonal selection the removal of daughter cells are performed, and these cells have receptors that respond to the body's own proteins as well as the most suitable mature cell proliferation, i.e., those with a greater affinity to the antigens (Coelho et al., 2013).

3 AIS NODE POSITIONING

Router Nodes positioning has been addressed in the literature by several researchers. (Cannons et al, 2008) propose an algorithm for positioning router nodes and determine which router will relay the information from each sensor. (Gersho and Gray, 1992), proposed one to promote the reliability of wireless sensors communication network, minimizing the average probability of sensor transmission error. (Shi et al., 2009) propose a positioning algorithm of multi-router nodes to minimize energy consumption for data transmission in mobile ad hoc network (MANET - Mobile Ad Hoc Network). The problem was modeled as an optimization clustering problem. The suggested algorithm to solve the problem uses heuristic methods based on the k-means algorithm. (Costa and Amaral, 2010) describe an approach for router nodes placement based on genetic algorithm which minimizes the number of nodes required for network routers, decreasing the amount critical nodes for all involved devices and the number of hops of the transmitted messages. 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 t 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. The stimulation of the B cells, corresponding to the set of routers, is defined by the affinity degree among B cells in the training of the network. In this paper, the role of the antigen is viewed more broadly as the entity that stimulates B cells. Thus, the function of the antigen takes into consideration possible missing paths to critical sensors, the number of times that a router is used and its proximity to sensors. The modeling of B cells affinity is the weighted sum of the three criteria that the positioning of each router will answer. The criteria are: fault degree of each router, number of times each router is used depending on the path and number of sensor nodes neighboring to each router. Process dynamics can be divided into two processes: network pruning and cloning, and node mutation of the network routers. In the pruning process, n_p router nodes that during a certain time failed to become useful to the network will be removed from it. The latter process is responsible for generating n_c clones of router nodes that were over stimulated. The clones may suffer mutations of two kinds:

(i) hypermutation – for positioning new elements in the network which are inversely proportional to the degree of stimulation of the router node selected and

(ii) net Mutation – for positioning the new information into the network in order to assure the new clones are neighbors of the selected clone (Poduri et al , 2006).

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.

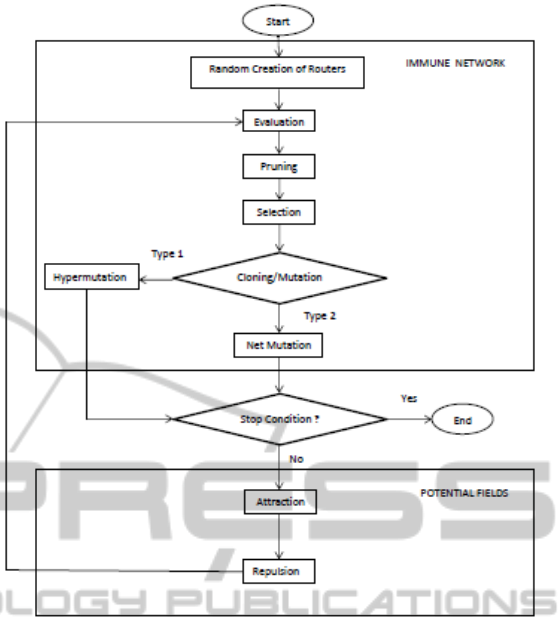

Figure 1: The proposed algorithm.

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 B cells to form a network.

Evaluation: Determination of the B 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 B cells to be cloned.

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

Mutation: Does the mutation of cloned cells.

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. It should be stressed that the affinity value is calculated for each router and comprises three parts. The first part provides the degree of fault of each network router - this affinity is the most important of all. It defines the value or importance each router has in the network configuration. This is done as follows: a router is removed from the network, and the number of paths that remain active for the sensors send information for the gateway is evaluated. If the number of active paths remaining after the node removal is small, the router node needs another nearby router to reduce their degree of fault. Furthermore, if the node suffers battery discharge or hardware problems, other paths to relay information should be guaranteed until the problem is solved. The second part relates to the number of times that each router is used in paths that relay the information from the sensors to the gateway. The greater the number of times it is used, more important is that router. The third part relates the number of sensor nodes neighboring to each router – one can say that the more sensor nodes neighbors, the greater the likelihood that it will become part of the way that the sensor needs to transmit your message to the gateway.

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 functionality of the developed algorithm. The configurations used in the simulation were motivated by oil & gas refinery automation applications. The first one called POSA consists of five network nodes, where node 1 is the gateway and nodes 2, 3, 4 and 5 are fixed sensors. The gateway has direct line of sight with all the network nodes as shown in Figure 2. The second scenario (POSB) considers a network with nine nodes, where node one is the gateway and the others are fixed sensors. As in scenario POSA, POSB has direct line of sight with all the network nodes as shown in Figure 3. For both configurations it will be considered that there is no connectivity among them, i.e. the distance between them will be greater than their operating range.

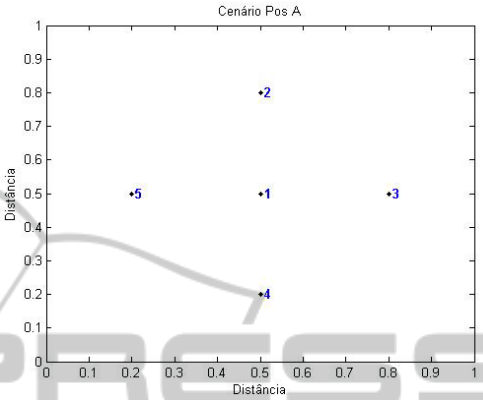

Figure 2: Sensors and gateway POSA configuration. (Legend: node 1:gateway; nodes 2 to 5: sensors).

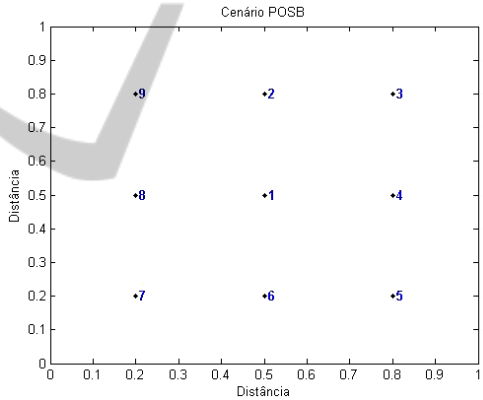

Figure 3: Sensors and gateway POSB configuration. (Legend: node 1:gateway; nodes 2 to 9 :sensors).

For the case study simulations considered, the goal is to get any two paths for each sensor to transmit the monitored sensor data to the gateway node. The operating range for both cases is 0.2, i.e. for both configurations there is no connectivity between any sensor and the gateway. Table 1 describes the parameters used in the case study 1. After completion of ten experiments, the best network configuration can be seen in figure 4, and the consolidations of the tests are shown in table 2. Figure 4 also shows that one of the paths from sensor node 3 to the gateway shows three jumps (3-7-8-1) i.e. the information had to be relayed by two routers to reach the gateway node. Regarding the degree of fault, all eight routers have 20 % degree of fault tolerance. This means that 80 % of the paths

from the sensors to the gateway continue to exist even after the removal of a node. With respect to the maximum number of routers used in terms of paths, the router node 8 is used twice in the paths 3-8-1 and 3-7-8-1. Consequently, this router will have a greater battery consumption than the others, which could make it stop working and be disconnected from the network. But even if that happens, there will still be a path (3-7-10-1) for node 3 to communicate to the gateway.

Table 1: Case study 1 – POSA configuration parameters.

Simulation Parameters	Values	Method
Number of generations	50	-
Initial number of Routers	10	-
Affinity	-	Fault Degree

Table 2: Network performance for case study 1.

Network	Min.	Av.	Max.	St. Dev.
No. of nodes	13	13,7	15	0,67
No. of routers	8	8,7	10	0,67
No. of critical sensors	0	0	0	-
No. a router is used	1	2,1	3	0,57

Case study 2 considers configuration POSB for the sensors and gateway. Table 3 shows the parameters used in the case study 2 simulation. The goal is still obtain at least two paths for each sensor and gateway but now the affinity criteria consider fault degree, number of times a router is used and number of neighbor sensors. After ten experiments the best network configuration is shown in figure 5 and the network performance is seen in table 4. Table 4 indicates that even using a low number of initial routers the algorithm was able to reach a positioning result meeting the goals and avoided again critical nodes. Figure 5 also shows that node 3 in the path 3-15-17-13-1 features four hops to the gateway. That means that the information sent by these devices will be delayed when received by the gateway node, since it will need to be relayed through three intermediate nodes. Regarding to the degree of fault, the intermediate node 22 has 22 % degree of fault, and all the other routers we have an index less than 22 %. Thus if node 22 is lost for device failure or end of battery results that information sent by sensor 5 will not reach the gateway. Regarding to the maximum number of routers used in terms of paths , router nodes 10 and 13 are used three times in the paths 3-15-17-13-1 , 3-26-13-1 , 4-13-1 , 9 -18-12-10-1, 9-24-10-1 and 2-11-10-1 .That means that these devices will have their lifetime reduced

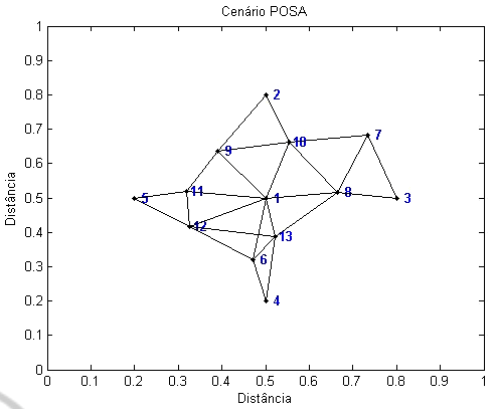

Figure 4: Node positioning for case study 1 in POSA configuration.

Table 3: Case study 2 – POSA configuration parameters.

Simulation Parameters	Values	Method
Number of generations	15	-
Initial number of Routers	3	-
Affinity	-	Failure Degree, No. of times a router is used and No. of neighbor sensors

Table 4: Network performance for case study 2.

Network	Min.	Av.	Max.	St. Dev.
No. of nodes	23	25,3	28	1,49
No. of routers	14	16,3	19	1,49
No. of critical sensors	0	0	0	-
No. a router is used	3	3,7	5	0,67

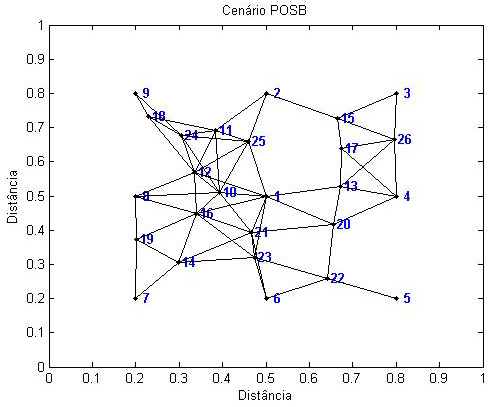

Figure 5: Node positioning for case study 1 in POSB configuration.

because their high levels of retransmission. As far as the number of sensors to neighboring routers is

concerned, routers 15, 19, 22 and 26 can relay the data sent by two sensors, and the sensors are also used with relays. This makes these sensors and routers consume more power, and as a result, battery runs out sooner.

This paper 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. Comparison between the results obtained in this paper and those known from the literature are not straightforward to produce since their criteria were not the same as ours. Our criteria considered as a top priority the fault tolerant aspect guaranteeing, for instance, in the case studies presented, at least two paths to the gateway for each sensor node. The affinity function, which works as an objective function, is multi-objective so several other objectives could be jointly considered. Another alternative could be to use some sort of workbench problem and try to compare other methods with ours, but the definition of a suitable workbench problem has issues which are difficult to deal with.

REFERENCES

Zheng, J., and Lee, M. J., 2006. *A Comprehensive Performance Study of IEEE 802.15.4*. *Sensor Network Operations*, IEEE Press, Wiley InterScience, Chapter 4, pp. 218-237.

Costa, M. S., Amaral, J. L.M., 2010. A tool for node positioning analysis in wireless networks for industrial automation. In *XVIII Automation Brazilian Congress*. Bonito, pp. 1521-1527, in portuguese.

Moyne, J. R. and Tilbury, D. M., 2007. *The Emergence of Industrial Control, Diagnostics, and Safety Data*. Proceedings of the IEEE, 95(1), pp. 29-47.

Cannons, J., Milstein, L. B., Zeger, K., 2008. An Algorithm for Wireless Relay Placement. *IEEE Transactions on Wireless Communications*.USA. Nov.2006. vol.8, n°11, pp. 5564-5574.

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.

Gersho, A., Gray, R. M., 1992. *Vector Quantization and Signal Compression*. Norwell, MA. Kluwer Academic Publishers.

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.

Coelho, P. H. G., Amaral, J. L. M. and Amaral, J. F. M., 2012. Node Positioning in Industrial Plants Wireless Networks. In *WES'12 International Conference on Communications, Rio Grande, R.S.,* in portuguese.

Shi, Y. , Jia,F., Hai-Tao, Y., 2009. An Improved Router Placement Algorithm Base on Energy Efficient Strategy for Wireless Network. In *ISECS International Colloquium on Computing, Communication, Control and Management (CCCM2009)*, pp. 421- 423.

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.

Poduri, S., Pattem, S., Krishnamachari, B.; Sukhatme, G., 2006. Controlled Deployments of Sensor Networks. In Press.

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*.