An Ecological Approach to Anomaly Detection: The EIA Model

Pedro Pinacho , Iván Pau , Max Chacón , and Sergio Sánchez

Abstract. The presented work proposes a new approach for anomaly detection. This approach is based on changes in a population of evolving agents under stress. If conditions are appropriate, changes in the population (modeled by the bioindicators) are representative of the alterations to the environment. This approach, based on an ecological view, improves functionally traditional approaches to the detection of anomalies. To verify this assertion, experiments based on Network Intrussion Detection Systems are presented. The results are compared with the behaviour of other bioinspired approaches and machine learning techniques.

1 Introduction

This paper proposes an artificial immune system (AIS) based on a population of evolutionary agents. The model is centered on the effect of environmental changes or perturbations on highly sensitive individuals, employing the concept of bioindicator [15]: that is, the quantification of this effect on the population of individuals in order to detect abnormalities. Because such an environment is the continuous representation of the characteristics of a monitored system, the model must be used for the detection of anomalies in any characterizable system based on a a parameter flow representing its state.

Anomaly detection is a solution to the problem of classification that consists of segregating objects in a set of different classes. In some cases, these classes are predefined and do not change over time. In more complex cases, classes may not be defined a priori, and may change over time. One of the more complex scenarios is Network Intrusion Detection Systems (NIDS). In this realm, the classifying algorithm must deal with at least two fundamental classes: normal traffic and intrusive traffic. These classes are not static, as they change due to the usual variation in the behavior of system users or the presence of a new or unknown attack. Hence, this scenario has been chosen to test the capacities of the classifier proposed in this paper.

The Artificial Indicator Species model (EIA in spanish) proposes an ecological approach, assuming that an agent population that plastically adapts to its

surroundings in order to subsist will develop learning skills, which is its structural modification in this context. This ecological approach is present in Varela's constructivist vision on the Biological Immune System (BIS) [26], which emphasizes self-affirmation and homoestatic potential. This vision is the inspiration for Nanas [20], which implements an adaptive network of terms used for filtering information. Unlike the approach set forth in this paper, it is based on a network and not on a population of agents.

The metaphor of the immune system has been widely used for the detection of intrusions in computer systems because they involve similar targets: the detection and elimination of agents that are not own/harmful/destabilizing. It is precisely this difference of concepts that has given rise to a prolific and diverse set [4] of hybrid techniques collectively called Artificial Immune Systems [10]. All these proposals seek to rescue capacities of identification, threat elimination, failure tolerance and adaptability of Biological Immune Systems through a series of proposals such as Formal Immune Network (FIN) [24], which is based on programmed cell death and cytokine-controlled immunization (messenger proteins), Clonal Selection (CLONALG), which posits a proliferation of detectors capable of detecting antigens and exploring them in order to enhance affinity by means of somatic hypermutation [5], Negative Selection (LISYS) [9] which is based on the maturation of T lymphocytes to produce immunological tolerance [12] and models based on the Jerne immune network [3]. There is evidence that these techniques do not deal with the change of normality in a consistent manner, while they also rely on models that are partial and not fully accepted [28]. Moreover, Bersini also shows that approaches based on the traditional conception of the immune system as a *defensive entity*, which is implicit in the foregoing techniques are incorrect, and it is encountering ever greater opposition among biologists [2]. For Bersini, the real contribution of the BIS model for engineering lies in the concept of endogenous double plasticity [6], which holds that a system adjusts structurally during its functioning in a continuous and plastic manner, integrating new elements and discarding old ones, with the change controlled by its internal dynamic. This is based on simple heuristics such as compensating for weak elements, maintaining diversity and eliminating redundancy, that is, maintaining balances through ecological mechanisms, which is the foundation of the present paper.

The approach in the EIA model possesses substantial operational advantages over the prevailing approach for developing NIDS, which is focused mainly on classifiers which relies on the use of recognized attack signatures or patterns, with the drawbacks of requiring constant updating to be useful, in addition to proving ineffective against unknown attacks [11]. The latter is one of the main points of interest in the development of AIS, which are closer to approaches based on the detection of anomalies. Although they do provide a solution to the problem of novelty attacks, they carry the drawback of being associated to a significant increase in false positives [7].

The structure of the model, its components and the functioning of the prototype elaborated with the multi-agent programming tool Netlogo [23] are presented

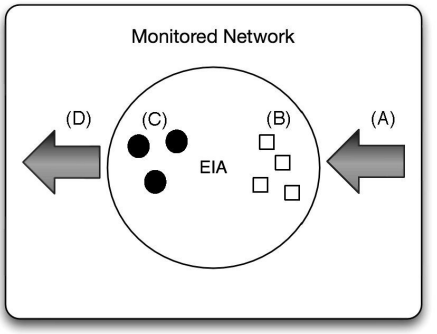

Fig. 1. General System Scheme

in Section II. Section III shows the procedure for transforming agents into bioindicators, and Section IV presents the adaptation of the model to be used as a classifier in the domain of information security. Section V describes the experiments and provides details on the algorithms used for comparison. Section VI gives the results, which were statistically validated with the Wilcoxon sign test [27]. Finally section VII sets forth the main conclusions of the paper.

2 Model

The general model, of which the EIA proposal is an anticipation, envisions the immune system as a symbolic entity that seeks to preserve or find new internal equilibria between chaos transitions generated by perturbations produced by attacks for this study. In this context, system learning is achieved through the progressive adaptation of its agents, which causes a continuous structural modification of the agent population by means of natural selection and the use of a mutation operator. Immunity is understood, in this scheme, as a cognitive system, owing to its recognition, learning and memory abilities [26].

The system model is structurally described in equation 1, where FADS is for *Flow Anomaly Detection System*, T, T is a bidimensional topology inhabited by a set of evolutionary agents, A is the set of agents and X is a set of particles consumed by agents and determined by the medium where the agents are inserted: that is, the system must be monitored.

$$FADS = \langle T, A, X \rangle \tag{1}$$

Figure 1, shows a schematic view of the general operation of the EIA model, which has the following stages:

- *Guest Characteristic Capture (A):* In the first phase, the system hears a continuous characteristics flow which represents the operation of the system under analysis.

- *Model Characteristic Input (B):* Subsequently, the characteristic flow is preprocessed, yielding observable characteristics in the same binary form $\alpha \in X$, which are inputted in topology T of the model.
- *Agent Exposure (C):* Adaptive agents $\beta \in A$ are exposed to elements of X, causing an increase or decrease of their energy, and with this strenghening, their reproduction or death.
- *Population Impact (D):* When observable characteristics (α) impact on agents, they generate effects that can be measured at a population level through two variables of interest: *population size* and *average energy* of the agent population, which are the basis for the developed classifier.

2.1 Artificial Bioindicators

The EIA model has been created with the multiagent programming tool Netlogo. Agents $\beta \in A$ are created, initially, with a random genetic configuration, with the expectation that the fittest will survive and generate decendents. Each agent has a structure $\beta = (\pi, \theta, \lambda)$, where $\pi \subset \Pi$ is the set of rules that determines the conduct of the agent β, θ corresponds to the genetic value of the agent and $\lambda = (\rho, \psi)$ determines the agent's position in the topology T, given by ρ, and the current energy of the same, as given by ψ.

Reproduction of agents is asexual and uses a mutation operator that acts on the vector described in Equation 2, carrying out a permutation between two elements of the vector. The importance of the genetic vector is that it determines the affinity of each agent with the environment. This affinity is constituted by a gene for each particle α of the existing n.

$$\theta = \left\{(g_0, g_1, \ldots, g_n) \middle| \forall g_k, g_j \, \langle (k \neq j) \Rightarrow (g_k \neq g_j) \rangle \right\} \tag{2}$$

When α impacts an agent, it becomes either food or poison, depending on the expression shown in Equation 3, which determines its nutritional value (NV). Where i is the index of gen g_k which represents particle α_k that has impacted the agent, ϕ represents the maximum nutrition that can be provided by a particle α and ϵ is a parameter that determines a linear nutritional loss applied owing to a lack of affinity with particle α.

$$NV = \phi - i\epsilon \tag{3}$$

Agents β are governed by the set of rules (π) described in Table 1, where (1) specifies that agents must achieve a minimum level of energy established by $ReproductionQualityOfLife$ (RQL) in order to generate descendants, in (2) it is specified that agents, when losing all their energy due to poisoning – that is, owing to a lack of affinity with particles α in circulation - are eliminated; in (3) agents have a baseline energy consumption determined by the variable $metabolism$ and in (4) agents are fed by all the particles impacting on them.

Table 1. EIA World Rules

Agents behavior rules (π)
(1) $(agent(\beta) \wedge energyMoreThan(\beta, RQL)) \Rightarrow birth(\beta^{'})$.
(2) $(agent(\beta) \wedge energyExhausted(\beta)) \Rightarrow kill(\beta)$.
(3) $agent(\beta) \Rightarrow energyReduce(\beta, Metabolism)$.
(4) $(agent(\beta) \wedge particle(\alpha) \wedge colision(\beta, \alpha)) \Rightarrow eat(\beta, \alpha)$.
World physics rules (ω)
$(i)\ observedParameter(x) \Rightarrow insert(\alpha_x)$
$(ii)\ (particle(\alpha) \wedge outOfRange(\alpha)) \Rightarrow remove(\alpha)$
$(iii)\ (particle(\alpha) \wedge exhausted(\alpha)) \Rightarrow remove(\alpha)$
$(iv)\ particle(\alpha) \Rightarrow LeftMove(\alpha)$

2.2 Topology and Particles

EIA corresponds to a model of artificial life that possesses a set of simple physical rules that regulate the behavior of particles α in the topology T.

The EIA topology $T = \langle E, \Omega \rangle$, is composed of E, to which all the cells in the topology belong, and by the world rules Ω, described in Table 1. The topology of the presented model is linear. Other topologies will be evaluated in future works. As observed in Figure 2, the topology corresponds to a 32x16 bidimensional grid. The rule (i) allows for the input of new particles in the topology when the corresponding characteristic has been observed in the network traffic being monitored; the rule (ii) eliminates a particle of the model when it outputs from the topology; rule (iii) eliminates particles that are exhausted due to the consumption caused by the collision with the agents and rule (iv) is the rule of movement which carries all the particles inserted in a random rightward position in the column (initial position) towards the left. This movement occurs once for each particle α from synchronic iteration of the model

3 Model Sensitization

The structures discussed and the rules on the basis of which they act in EIA constitute a system comprised of an agent population that adapts to the normality of a supervised system. It would be of interest to observe the population reacting in a sensitive and quantifiable manner to disorders caused by abnormalities in the observed system. Hence, the parameters in the model were adjusted and agents were made highly sensitive to these disorders, thus becoming bioindicators.

The flow generation function was used to yield a sequence of variations in the input vectors, thus testing each of the parameters of the model in order to find values that would lend greater sensitivity to the agent population. Tested values

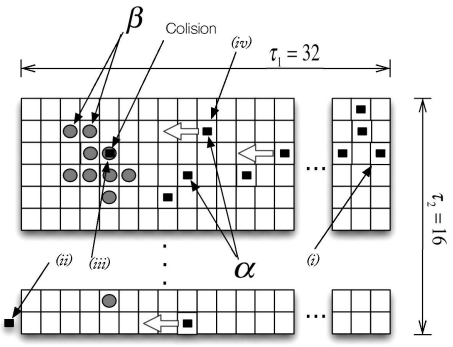

Fig. 2. EIA

in EIA parameters correspond to a variation in values that sensitize agents previously found in an experimental manner. This procedure increased the general sensitivity to flow variations of the EIA model from an average of 35% to 62% in the tests performed.

Figure 3 shows the evolution of the agent population, following the adjustment of these parameters, from their creation to their exposure to an attack. At moment 0, an initial population of 300 agents is created with random genetic vectors. These agents are exposed to habitual network traffic, thus leading to an adjustment consisting of the death of unfit agents and a reduction of the population to fewer than 50 individuals. Subsequently, the most fit agents proliferate and generate descendance by mutation. Until iteration 5570, there is an increase and stabilization of the agent population with an incidence of fractal noise that is intrinsic to ecological systems [19]. In iteration 5570, a probe attack with Satan[1] occurs, causing a significant fall in the size of the population, that is, a quantifiable deviation in one of the model's variables of interest, which is the basis for using the model as a classifier.

4 The Classifier

Once the agent population is sensitized to any perturbations in the environment (achieved through adjustments in model parameters), attention must center on change in the emerging structure established: that is, on the repercussions of environmental changes on the population level. This is achieved by means of monitoring the aforementioned variables of interest.

The variables of interest population size and average population energy exhibit noise in their behavior. Hence, a measurement of their trends for use as discriminators should be considered, and such variables are therefore transformed into classifiers through the incorporation of sliding windows and thresholds with the following parameters:

[1] SATAN (Security Administrator Tool for Analyzing Networks).

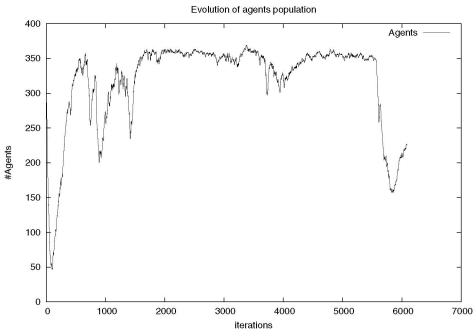

Fig. 3. Evolution of Agents Population

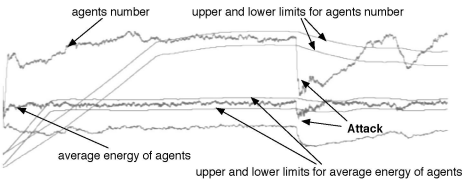

Fig. 4. sliding windows working on Netlogo

Table 2. Detected Characteristics

Detected Characteristics (α)
IP reserved bits, MF, DF, Urg, Ack, Reset, Syn, Fin, Telnet, SSH, FTP, Netbios, rlogin, RPC, NFS, Lockd, NetbiosWinNET, Xwin, DNS, LDAP, SMTP, POP, IMAP, HTTP, SSL, px, Serv, Time, TFTP, NNTP, NTP, lpd, Syslog, SNMP, bgp, Socks

- *Length of sliding windows:* This parameter sets the number of past values used in calculating the current average of the variables of interest. This corresponds to the point of reference used by higher and lower tolerange ranges, which may be observed in Figure 4.
- *Tolerance bandwidths:* Determines the distance of the bands accompanying the variable of interest. If the variable of interest exceeds the upper or lower limit owing to more iterations than those established in the *classifer alarm threshold*, an intrusion alarm is declared.
- *Classifer alarm threshold:* Sets the maximum successive iterations the variables of interest can exceed a tolerance range without triggering an alarm.

These parameters are adjusted in accordance with the domain of computer security, particularly the development of NIDS systems. These systems can be understood as classifiers capable of detecting an attack based on an analysis of

network traffic, where this traffic is a continuous flow of data that is captured with sniffing techniques, that is, the capture of all accessible network traffic at the point of connection In this scenario, the flow characterizing the system under study (i.e., the monitored network) is used to feed the agent population in the EIA model package by package, based on information from the transmission and network layers of the TCP/IP stack. This is achieved by transforming through pre-processing forty characteristics of network traffic specified in Table 2, thus allowing the incorporation of their representations in the EIA model by means of particles (α).

The data for running this calibration process were extracted from different sources: samples of normal traffic were obtained from the network of the Department of Information Technology of the University of Santiago de Chile, while the security tools NMAP and Nessus were used to generate hostile traffic. Specifically, these tools generated probe and denial-of-service (DoS) attacks, respectively.

Probe, according to DARPA [18] are related to remote reconnaissance activities carried out by intruders prior to an attack, while DoS attacks consist of any activity aimed at preventing the delivery of a computer service. From this point of view, any attack on the availability of a system falls in this latter category.

Selection of classifier parameters posited a classifer based on the variable of interest agent population size, a second based on the average energy of the population and, finally, a unifying classifier based on the best parameters of the two first classifiers, but recalibrating the alarm threshold. The adjustment was made with the Receiver Operating Characteristic Curves (ROC) technique [8].

To identify the best classifier, a comparison was made of areas under the ROC curves (AUC). These areas have values between 0.5 and 1, where 1 represents a perfect classification and 0.5 signifies complete discriminatory incapacity. Experiments with the results observable in Figure 5, determined that the area under the curve (AUC) of the unified classifer (0,8149) is greater than both that based on population size (0,7860) and that based on average energy (0.7664). Hence, it is selected for the execution of comparative tests based on traffic for a standardized benchmark. The best classifier parameters found may be observed in Table 3. Because the algorithm is non-deterministic, all tests were performed 10 times, with curves generated by means of Bezier approximations.

Table 3. Classifier Parameters

Parameter	Value
Length of sliding window (Agents)	900
Tolerance bandwidth (Agentes)	2
Length of sliding window (Energy)	2800
Tolerance bandwidth (Energy)	0
Joint alarm threshold	200

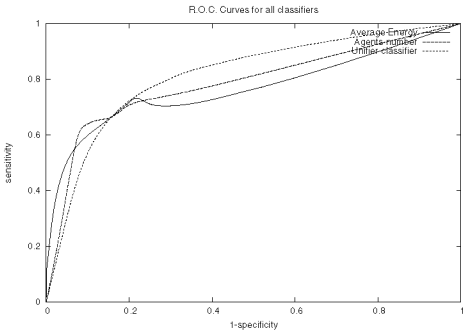

Fig. 5. Receiver Operating Characteristic Curves for all Classifiers

5 Experiments

The experiments specified in this section were posited to verify that a classifier based on notions of ecological systems can attain operational advantages over other automatic learning systems in the classification problem in intrusion detection systems by adaptating to changes in normal conditions and detecting innovative attacks. Comparisons were made with other bio-inspired classification techniques used successfully to develop NIDS, and such techniques were used to verify skill in detecting known and unknown threats.

5.1 Experiment Data

Tests of the EIA model and classifiers in comparison were performed with the widely used DARPA'98 data set. Use was discounted of KDD'99 data, which are considered to be of questionable validity and usefulness [21] , and also poor for the evaluation of anomaly detector systems [25].

5.2 Algorithms Evaluated

The classifier based on the EIA model was subjected to comparative tests to three other classifiers based on biological metaphors as described below:

- *Artificial Neural Network (ANN):* Use of a multilayer perceptron is being considered owing to its good results in the implementation of intrusion detection systems [16]. The network was trained with backpropagation and Levenbeg-Marquard because these reduce the number of false positives [17]. The quantity of neurons in the hidden layer was calculated according to [22] and then adjusted in a calibration process, leading to assignment of 16 neurons in the hidden layer based on an correctness criterion, with the use of 54 input characteristics from the TCP/IP package headings.

- *Formal Immune Network (FIN):* This proposal of immunocomputing (IC), like the neural network, can be considered to fall within the field of computational intelligence. FIN proposes the generation of a Euclidean multidimensional space (FIN space) in which a training process based on application of a discrete tree transform (DTT) [1] and/or a singular value descomposition (SVD) [13] incorporates input data and its initial space, which is optimized to form a set of class representatives for representation called cytokines, following a process of apoptosis and immunization explained in [24]. These cytokines operate according to a proximity principle in the FIN space to determine the class of data reviewed when mapped in the space with the DTT algorithm.
- *Modified Formal Immune Network (FIN+):* The test was conducted against a modified version of FIN (FIN+) developed for this comparation. By incorporating the concept of time and uncertainty, it generates temporary groupings, detecting regions of space with quick growth for classification as attacks, thus improving performance against unknown attacks of the original algorithm.

5.3 Design of Experiments

To evaluate the behavior of classifiers in changing scenarios and in detection of new/unknown attacks. Described algorithms are measured and compared in terms of false positives (FP) or type I errors and correctness determined by Equation 4, where (TP) represents True Positives and (TN) represents True Negatives. The results were statistically validated with the Wilcoxon sign test.

$$Correctness = \frac{(TP + TN)}{n} \tag{4}$$

The tests were divided into two groups: known attacks and unknown attacks. Tests with known attacks were executed by subjecting the classifiers ANN, FIN and FIN+ to training that includes the attacks to which they will be exposed. Further, the unknown attack group is based on attacks not included in the training sets of classifier algorithms: this distinction does not apply to the EIA-based algorithm because the latter is not trained with attacks, but only exposed to normal traffic of 3000 packets, a time that has been empirically shown to be sufficient for their adaptation or the stabilization of the agent population.

6 Results

Table 4 shows the average FP values and the correctness achieved by the classifier algorithms for tests with known and unknown attacks. It may be observed in the table that for known attacks, EIA (15.56%) yields fewer false positives than other classifiers, with the closest being the modified version of the Tarakanov-Iturbe algorithm (FIN+), with 23.38%, a significant difference ($p \leq 0.05$). For the same type of attacks, EIA achieves better average correctness than the three

Table 4. Main Results

	Known Attacks		Unknown Attacks	
Classifier	FP	Correctness	FP	Correctness
EIA	0.1556	0.7848	0.1556	0.7848
FIN	0.26	0.7017	0.2923	0.6756
FIN+	0.2538	0.6728	0.2762	0.6798
ANN	0.3097	0.6670	0.3477	0.6284

classifiers with which it is compared; but it achieves a significant advantage with ANN and FIN ($p \leq 0.05$), although not with FIN+, of which it does not deliver a significant distance.

In the unknown attacks scenario, EIA (15.56%) yields significantly better results in terms of false positives than the other three classifiers ($p \leq 0.05$)), with the closest being the result of FIN+ (27.62%). The same result repeats in the results of average correctness marks, where EIA attains 78.48% against FIN+ (67.98%), thus attaining a result that is better than the other three by $p \leq 0.05$. The EIA model achieves a specificity of 86%, sensitivity of 95%, and precision of 86%.

6.1 Other Tests of EIA

The EIA classifier was subjected to further tests to check the consistency of the results, as the non-deterministic algorithm means that the results may differ from one experiment to another. Verification was perform by means of tests on characteristic attacks of each of the categories in the DARPA '98 set, which are: DoS, R2L, U2R and Probe. Where R2L (Remote to Local) refers to a category of attacks in which the intruder seeks to gain access to a computer system remotely and U2R (User to Root) refers to an unauthorized attempt to increase privileges.

In Table 5 it may be observed that EIA consistently detects practically all test series in DoS, R2L and probe attacks, whereas it cannot detect U2R attacks as easily, as it successfully did so in only half the experiments. This result is consistent with the general behavior of EIA, where it more easily detected DoS and Probe attacks. This is explained by the fact that variables based on the EIA agent population possess a certain inertia owing to the use of a sliding window and it reacts more readily to more extensive perturbations such as those caused by port scanning or flood attacks in the categories of Probe and DoS, respectively.

In terms of attacks, EIA detected in the first instance 35 of 47 attacks in the DARPA'98 set (74%). Review of undetected attacks revealed that none had sufficient length to activate the classifier because the parameter adjustment based on the ROC curve indicated that the best value of the classifier alarm threshold is 200. Thus, if the attack is not part of a packet trace (with normal background traffic) that is longer than 200, it does not trigger an alarm in the classifier. This

Table 5. Classifier Consistency

Category	Attack	Detections
DoS	Neptune	99/100
R2L	Dict	99/100
U2R	FFB	50/100
Probe	SATAN	100/100

may be related to the fact that the ROC calibration was performed with probe and DoS attacks of a moderate length. In later tests, in which the length of attacks was determined arbitrarily in order to complete at least the 200 packets necessary to sensitize the model, 11 of 12 attacks were detected. It should be noted that non-detection of these attacks in the tests did not significantly affect the comparative results owing to their minor presence in packet terms in the test data set of DARPA' 98.

7 Conclusions

This article provides a report on the proof of concept of a new "Flow Anomaly Detection System" (FADS) in development. The article includes the results of a set of experiments to show the features of the proposal and its applicability.

The analysis of the results verifies that it is feasible the creation of a population of evolutionary agents sensitive to environmental conditions that when subjected to stress can act as a classifier. In this way it is shown that these systems coincide with the biological evidence that the system's sensitivity to environmental changes increases when the genetic diversity of the species (agents) decreases.

When subjected to a complex problem of classification, the model developed has advantages over other bioinspired techniques traditionally used in the problem of intrusion detection network. The most important advantage obtained is the reduction of false positives where the technique of artificial indicator species (EIA) improves the results of three common indicators of both known and unknown attacks. The proposal has also shown competitive in terms of accuracy when attacks are known and even better than the other techniques when the attacks are unknown.

The classifier based on EIA proposes that learning by continuous adaptation has advantages over the machine learning techniques tested (FIN and ANN). Additionally it is shown that can outperform an algorithm with capabilities of online learning such as FIN+.

EIA is the first step in the project of developing a homeostatic control system. The main goal of the homeostatic control system is not to have separate stages of training and production but a unique dynamic and continuing stage to stabilize the host system where it is inserted, facilitating the maintenance of the whole system.

The use of bioindicators respond to partial advance of the system, which tackles the sensing and adjustment of the population of agents. In this context, it is necessary to obtain readings of the population changes, useful model to return to the current inability of the agents car modified their environment. For this reason, the next steps of this project oriented to allow the changes impacting the population of agents into the environment through a continuing dialogue achieved through its structural coupling [14].

References

1. Atreas, N., Karanikas, C., Tarakanov, A.: Signal Processing by an Immune Type Tree Transform. In: Timmis, J., Bentley, P.J., Hart, E. (eds.) ICARIS 2003. LNCS, vol. 2787, pp. 111–119. Springer, Heidelberg (2003)
2. Bersini, H.: Self-assertion versus self-recognition: A tribute to Francisco Varela. In: Timmis, J., Bentley, P.J. (eds.) Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS), pp. 107–112. University of Kent at Canterbury Printing Unit, University of Kent at Canterbury (2002), http://www.aber.ac.uk/icaris-2002
3. de Castro, L., Von Zuben, F.: ainet an artificial immune network for data analysis. In: Publishing, I.G. (ed.) Data Mining: A Heuristic Approach, pp. 231–259. Idea Group Publishing (2001)
4. Coutinho, A.: A walk with francisco varela from first- to second- generation networks: In search of the structure, dynamics and metadynamics of an organism-centered immune system. Biological Research 36(1), 17–26 (2003)
5. Cutello, V., Narzisi, G., Nicosia, G., Pavone, M.: Clonal Selection Algorithms: A Comparative Case Study Using Effective Mutation Potentials. In: Jacob, C., Pilat, M.L., Bentley, P.J., Timmis, J.I. (eds.) ICARIS 2005. LNCS, vol. 3627, pp. 13–28. Springer, Heidelberg (2005)
6. Dasgupta, D.: Artificial immune systems and their applications. Springer (1998)
7. Estevez-Tapiador, J.M., Garcia-Teodoro, P., Diaz-Verdejo, J.E.: Anomaly detection methods in wired networks: a survey and taxonomy. Computer Communications 27(16), 1569–1584 (2004)
8. Fawcett, T.: An introduction to ROC analysis. Pattern Recognition Letters 27(8), 861–874 (2006), rOC Analysis in Pattern Recognition
9. Forrest, S., Perelson, A., Allen, L., Cherukuri, R.: Self-Nonself Discrimination in a Computer. In: Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy, pp. 202–212 (1994); IEEE, Comp. Soc.; IEEE, Comp. Soc., Tech. Comm. Secur. & Privacy; Int. Assoc. Cryptol. Res. (1994); 1994 IEEE-Computer-Society Symposium on Research in Security and Privacy, Oakland, CA, May 16-18 (1994)
10. Glickman, M., Balthrop, J., Forrest, S.: A machine learning evaluation of an artificial immune system. Evolutionary Computation 13(2), 179–212 (2005)
11. Greitzer, F.L., Moore, A.P., Cappelli, D.M., Andrews, D.H., Carroll, L.A., Hull, T.D.: Combating the insider cyber threat. IEEE Security & Privacy 6(1), 61–64 (2008)
12. Harmer, P., Williams, P., Gunsch, G., Lamont, G.: An artificial immune system architecture for computer security applications. IEEE Transactions on Evolutionary Computation 6(3), 252–280 (2002)
13. Horn, R., Johnson, C.: Matrix Analysis. Cambridge University Press (1986)

14. Humberto Maturana, F.V.: El Arbol del Conocimiento. Editorial Universitaria, Santiago (1976)
15. Jeffrey, D.W., Madden, B.: Bioindicators and environmental management. Academic Press, London (1991)
16. Kukielka, P., Kotulski, Z.: Analysis of Different Architectures of Neural Networks for Application in Intrusion Detection Systems. In: Ganzha, M., Paprzycki, M., PelechPilichowski, T. (eds.) International Multiconference on Computer Science and Information Technology (IMCSIT), Wisla, Poland, October 20-22, vol. 1 and 2, pp. 752–756. IEEE (2008)
17. Linda, O., Vollmer, T., Manic, M.: Neural Network Based Intrusion Detection System for Critical Infrastructures. In: IEEE International Joint Conference on Neural Networks (IJCNN), Int. Neural Network Soc., Atlanta, GA, June 14-19, vol. 1- 6, pp. 102–109 (2009)
18. Lippmann, R., Haines, J.W., Fried, D.J., Korba, J., Das, K.: The 1999 DARPA offline intrusion detection evaluation. Computer Networks-the International Journal of Computer and Telecommunications Networking 34(4), 579–595 (2000)
19. Halley, J.M.: Ecology, evolution and 1f-noise. Trends in Ecology & Evolution 11(1), 33–37 (1996)
20. Nanas, N., de Roeck, A.: Autopoiesis, the immune system, and adaptive information filtering. Natural Computing 8, 387–427 (2009), doi:10.1007/s11047-008-9068-x
21. Olusola, A.A., Oladele, A.S., Abosede, D.O.: Analysis of KDD '99 Intrusion Detection Dataset for Selection of Relevance Features. In: Ao, S.I., Douglas, C., Grundfest, W.S., Burgstone, J. (eds.) World Congress on Engineering and Computer Science, Int. Assoc. Engn., San Francisco, CA, October 20-22. Lecture Notes in Engineering and Computer Science, vol. 1 and 2, pp. 162–168 (2010)
22. Haykin, S.O.: Neural Networks and Learning Machines, 3rd edn., new york edn. Prentice Hall (2009)
23. Sklar, E.: Software review: NetLogo, a multi-agent simulation environment. Artificial Life 13(3), 303–311 (2007)
24. Tarakanov, A.O.: Immunocomputing for intelligent intrusion detection. IEEE Computational Intelligence Magazine 3(2), 22–30 (2008)
25. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.: A detailed analysis of the KDD CUP 99 data set. In: IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009, pp. 1–6 (July 2009)
26. Varela, F.: El Fenómeno de la Vida, 2nd edn. OCEANO, Santiago de Chile (2000)
27. Wilcoxon, F.: Indicidual Comparisons by Ranking Methods. Biometrics Bulletin 1(6), 80–83 (1945)
28. Wu, S.X., Banzhaf, W.: The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing 10(1), 1–35 (2010)