PhD proposal for MAP-i doctoral program

November 2010

Title: *On the application of Artificial Immune Systems for anomaly detection.*

Supervisors: Manuel Eduardo Correia (mcc@dcc.fc.up.pt)and Mário Antunes (mario.antunes@estg.ipleiria.pt)
CRACS-INESC LA, Department of Computer Science, Faculty of Science, Oporto University

The functions of anomaly detection and self/non-self distinction embodied by the Vertebrate Immune System (IS) have been a very attractive source of inspiration for the development of innovative Artificial Immune Systems (AIS) [5] applied within the context of anomaly detection [7]. The two most popular immunological theories that have been used thus far for the deployment of effective anomaly detection AIS frameworks are Negative Selection (NS) and Danger Theory (DT) [7]. Despite the promising results achieved thus far, they proved to have some well documented difficulties in dealing with real world problems [7].

More recently, other promising immunological theories have been applied for the development of new AIS anomaly detection frameworks. One of such theories is the Tunable Activation Threshold (TAT) theory, which postulates that self tolerance and non-self discrimination is produced by the tunable adjustment of immune cells activation thresholds on some well known enzymatic levels [6, 4].

In the past three years we have developed a generic and context-independent AIS framework based on TAT [2, 1, 3]. This framework embodies an immunological metaphor between immune cells and artificial counterparts, as well as the adopted model. We have also made extensive effectiveness tests on several problem domains, for example by processing data sets comprised of real-world computer network traffic and have, for this case, compared the AIS performance with one of the most commonly used signature-based IDS; the Snort-IDS. The promising results obtained thus far motivated us to propose the following research activities:

1. Research innovative pre-processing methodologies for network traffic that could improve TAT anomaly detection performance.
2. Extend TAT processing for other application domains where we have already made some experiments with TAT, like email spam detection and text classification.
3. Fine tune the TAT adopted model, namely (1) New ways of calculating the signal each T-cell receives in its interactions with the environment (i.e. network traffic or email messages) and (2) explore and evaluate several new affinity metrics for the simulator.
4. Explore new methodologies for the optimization of the simulator run-time parameter set.
5. Develop TAT-AIS as a plug-in for the Snort-IDS system.
6. Take advantage of multi-core architectures by paralysing the cell simulator run-time cycles.
7. Develop new strategies for the deployment of TAT embedded within an ensemble context composed by other machine learning approaches, like for example SVM. We have already tried this approach on the free text classification domain, with very promising results.

Bibliography

[1] M. Antunes and M. Correia. Self tolerance by tuning t-cell activation: an artificial immune system for anomaly detection. In Springer LNICST, editor, *Bionetics*, 2010.

[2] M. Antunes and M. Correia. Temporal Anomaly Detection: an Artificial Immune Approach Based on T-cell Activation, Clonal Size Regulation and Homeostasis. *Advances in Computational Biology - Book series*, 680:291–298, 2010.

[3] M.J. Antunes and M.E. Correia. An Artificial Immune System for Temporal Anomaly Detection Using Cell Activation Thresholds and Clonal Size Regulation with Homeostasis. In *Bioinformatics, Systems Biology and Intelligent Computing, 2009. IJCBS'09. International Joint Conference on*, pages 323–326. IEEE, 2009.

[4] J. Carneiro, T. Paixão, D. Milutinovic, J. Sousa, K. Leon, R. Gardner, and J. Faro. Immunological self-tolerance: Lessons from mathematical modeling. *Journal of Computational and Applied Mathematics*, 184(1):77–100, 2005.

[5] L.N. de Castro and J. Timmis. *Artificial Immune Systems: A New Computational Intelligence Approach*. Springer, 2002.

[6] Z. Grossman and WE Paul. Adaptive cellular interactions in the immune system: The tunable activation threshold and the significance of subthreshold responses. *Proceedings of the National Academy of Sciences*, 89(21):10365–10369, 1992.

[7] J. Kim, P.J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross. Immune system approaches to intrusion detection - a review. *Natural Computing*, 6(4):413–466, 2007.