Artificial Immune Systems – AIS as Security Network Solution

Edward Guillen[1] and Rafael Paez[2]

[1] Military University "Nueva Granada" , Bogota, Colombia
edward.guillen@unimilitar.edu.co
[2] Javeriana University, Bogota, Colombia
paez-r@javeriana.edu.co

Abstract. Network security attacks have a dynamical performance and their rate of change is commonly faster than protection technologies. The defense mechanisms usually act with reactive non proactive solutions in a non-self learning procedure. However, bio-inspired methods such as AIS could give a new dynamical method to defend entire data network from malicious attacks. This short paper briefly analyzes the possible use of AIS in secure network architectures to be implemented with future research projects.

Keywords: AIS, BIS, Network Security.

1 Introduction

The Artificial Immune Systems –AIS began in the early 90s as a branch of the Computational Intelligence –CI [1], and their main goal is to develop computational methods inspired by Biological Immune Systems –BIS in order to solve computational problems [2].The natural characteristics of BIS are their ability of pattern matching by the recognition of foreign cells that are mixed with the cells that belong to the body [3]. Other important features of BIS includes: feature extraction, memory, learning, and distributed nature [2]. When applying these concepts to computational problems, it is possible to find interesting solutions with the analogies found on BIS, for example: computer security applications, machine learning, detection in time series, anomaly detection, and chemical spectrum recognition. [4], [5], [6], [7], [8], [9]. We want to focus the AIS solutions into security applications by using analogies between BIS and the behavior of malicious attacks over telecommunication networks, in order to propose investigation projects to solve the challenge of protecting information.

2 Security Threats and BIS

Malicious software has a similar behavior than its biological counterpart. Trojan horses get into computer network by simulating a trustable behavior and turns into

J. Suzuki and T. Nakano (Eds.): BIONETICS 2010, LNICST 87, pp. 680–681, 2012.

malicious application inside the network. Worms can act by a mechanism of self-replication affecting the protection system and creating backdoors for the entrance of more dangerous attacks. Rootkits help malware to remain hidden. A bug is an error into the normal function of a system. A Botnet acts in a highly distributed system with a well synchronized performance in order to achieve a massive attack.

In the BIS, the central lymphoid organs generate immune cells and include bone marrow and the thymus [2]. There are a wide range of immune cells with different task in order to act in an immune response. Examples of these cells are stem cell, Lymphocytes, B and T cell progenitor, Natural killer cell, Neutrophil, Eosinophil and so on. New network security architecture should have a structure that could produce digital cell detectors for an entire network and not just a passive detection.

It is possible to map pathogens and antigens with malware and network attacks, immune cells with detectors, proteins with strings, immunological response with elimination strategies [4].

3 Conclusion

With AIS, it is possible to propose an interactive security scheme, not only at the final equipment but also in a Bio-inspired complete network defense architecture to be integrated with classical and new security appliances.

References

1. Dasgupta, D.: Advances in Artificial Immune Systems. IEEE Computational Intelligence Magazine (November 2006)
2. Dasgupta, D., Nino, L.F.: Immunological Computation, Theory and Applications. CRC Press, Boca Raton (2009)
3. Engelbrecht, A.: Computational Intelligence: An Introduction, 2nd edn. John Wiley & Sons Ltd., England (2007)
4. 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)
5. Zhou, X.: Evolutionary Algorithm and its Application in Artificial Immune System In: The Second International Symposium on Intelligent Information Technology Application (2008)
6. Dasgupta, D., Forrest, S.: Novelty Detection in Time Series Data using Ideas from Immunology. In: ISCA 5th International Conference on Intelligent Systems, Reno, Nevada, June 19-21 (1996)
7. Dasgupta, D.: Using Immunological Principles in Anomaly Detection. In: The Artificial Neural Networks in Engineering (ANNIE 1996), St. Louis, USA, Nov. 10–13 (1996)
8. Cao, Y.D., Dasgupta, D.: An Immunogenetic Approach in Chemical Spectrum Recognition. In: Ghosh, Tsutsui (eds.) Advances in Evolutionary Computing, ch. 36. Springer-Verlag, Inc. (January 2003)
9. Timmis, J., Neal, M., Knight, T.: AINE: Machine Learning Inspired by the Immune System. IEEE Transactions on Evolutionary Computation (June 2002)