On the Deployment of Artificial Immune Systems for Biometrics

Ruben Krishnamurthy[1], Kenneth Revett[2], and Hossein Jahankhani[1]

[1] University of East London
School of Computing & Technology
University Way
Beckton
London E15 2RD
ruben.krishnamurthy@gmail.com
h.jahankhani@uel.ac.uk
[2] Faculty of Informatics and Computer Science
British University in Egypt
El Sherouk City
Egypt
Ken.revett@bue.edu.eg

Abstract. Artificial immune systems (AIS) are a computational metaphor based on biological implementations of immune systems. Natural immune systems are capable of performing computation based on several properties that they possess. Immune systems are capable of adapting to new stimuli – they respond appropriately to novel stimuli, and they can remember previous encounters with stimuli. The processes which natural immune systems utilise are a combination of cellular and humoral responses – which act independently and in concert to perform stimulus identification and eradication, with minimal impact on the host. This provides an overview of artificial immune systems – which attempt to implement the basic functionality of natural systems. The basic properties and their interrelations are described in this paper – which is a prelude to their application in the context of biometrics. It will be demonstrated that the AIS approach is both a natural and potentially very effective approach to providing biometric security within a range of modalities.

Keywords: artificial immune systems, biometrics, computer security, distributed systems, natural computation.

1 Introduction

Artificial Immune System (AIS) is a new branch of computer science which uses the natural immune system as a metaphor for solving computational problems. AIS detect unusual/suspicious or rare events by using the ideology of the Immune system. AIS can be used for various applications namely Machine Learning (ML), Computer Security, Fault detection, behaviour of robots and for Novelty detection. A Pathogen is any agent could be virus, bacterium that may cause trouble. The Immune System is our primary defence against pathogens and it consists of nonspecific and specific

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 126–130, 2012.

defences. Non Specific Defences are the body's first line against any disease. Their normal function is to guard against all infections regardless of their cause. Specific Defences are attempts generated by the body to defend itself against certain pathogens.

2 Role of Immune Systems

One of the main role of the Immune System is to protect our bodies from infection and operating via two non specific lines of defence barriers and general attack namely and later via specific line of defence which entails the primary immune response whose role is to launch a response to invading pathogens and the secondary immune response whose role is to remember the past encounter which leads to a faster response the second time the same attack happens. The body's most important nonspecific defence is the skin, unbroken skin provides a continuous layer that protects the whole body. The sweat and oil glands at the surface of the skin produces a salty and acidic environment that kills the bacteria and other microorganisms. An infection occurs when a small portion of the skin is normally broken or scrapped off.

2.1 Second Line of Defence

When pathogens do get past the skin and mucous membranes and enter the body, the second line of defence takes an active role, triggered by the process of injury to tissues in the body. These injured cells release a protein called Histamine which then starts a process called the Inflammatory Response. Histamine normally increases the blood flow to the injured area and hence increases the permeability of the surrounding capillaries hence resulting in fluids and White Blood Cells (WBC's) leaking into tissues nearby from the blood vessels. Phagocytes engulf and destroy the Pathogens. If after all these lines of defence a pathogen is still able to get past the body's non specific defences, the Immune System (IS) would then react with specific defences that attack the disease causing agent and this is called the Immune Response (IR). An Antigen is known as a substance that triggers the specific defences of the Immune System. An Antigen is also a substance that the WBC identifies as not belonging to the body.

3 Algorithms

3.1 Negative Selection Algorithm

Forrest et al in [1] proposed an algorithm which is based on the biological negative selection principle. The algorithm is developed to detect anomalies in a set of strings which could be changed in the checksum and length which is done by using malicious codes or programs like a virus. A procedure called censoring is done first where the protected string is split into substrings which then form a collection S of Self (Substrings). The next step is to generate random strings R0. These randomly generated strings which match self are then eliminated and those which do not match any strings of S become a member of the detection collection called R – repertoire. Once this repertoire is produced, the monitoring phase is then started whereby the

match is done continuously from S against those in R. The effect of negative selection is to make a two-class problem a one-class problem. When the randomly generated pool of antibodies are culled (when they match the host antigens too strongly), only those antibodies with minimal reactivity will remain for subsequent maturation. If the mature antibodies respond to an unseen antigen, then one can as assume that the antigen was not from the host [2]. This antigen should then be considered for removal if this occurred in the context of a classic human immune system.

3.2 Clonal Selection Algorithm

This algorithm is modelled on the B-Cell mechanism. Naive B-Cells circulate in the blood and the lymphatic organs. Once the receptors of such a B-Cell match to an antigen, they proliferate quickly and they also change to attain a better matching value. Those B-Cells which have attained better matching proliferate again and again hence producing the best matching B-Cells. The induced changes are implemented as mutations, which serve to enhance the population of responding cells to the antigen. The rate of mutation within the immune system is much higher than the normal cellular mutation rate – this provides the search and sensitivity features of an adaptive immune system [3].

3.3 Immune Genetic Algorithm

This algorithm is based on a search technique mainly used in computing to determine approximate or true solutions, and also for optimization and search problems. A typical Genetic Algoritm first requires a genetic representation of the solution domain and secondly a fitness function for evaluating the solution domain. This standard representation is done via a bit array. The fitness function is dependent on the problem and measures the quality of the represented solution. Once both the genetic and fitness functions are defined, the Genetic Algorithm then initializes a population of solutions randomly then improving it thorough repetitive application of mutations, crossovers and selector operators. One main draw back with this algorithm was that it was not very good in local searches and is good with global search [4]. To overcome this problem Chun et al [5] proposed a new algorithm, which was based on the genetic algorithm whereby the antigen and the antibody are the objective functions and the solution and the affinity between an antibody and the antigen is the solution fitness. This method mainly improves the selection operator to produce a very good global search.

4 Applications

4.1 System Security

One of the most common application areas for AIS is in the deployment of intrusion detection systems (IDS). An intruder is an entity which attempts to acquire computing resources without proper authorisation. There are two basic forms of intrusion detection: signature and anomaly detection. The former deploys a ‘typical’ template for an intruder – the format is acquired through a supervised training approach in which hackers are asked to attempt to hack into the system. In anomaly detection, any

behaviour which deviates from typical behaviour is flagged as a possible intrusion. Anomaly detection is more likely to lead to large false positives, while a signature based approach tends to lead to increased false acceptance rates. Both types of IDS can be implemented using an AIS based approach. The antigen is the series of system calls that a user process generates during interaction with the host system. The antibodies are deployed to recognise 'typical' system calls. Those that are not recognised could be considered suspicious and further action must be undertaken to determine if this is a real threat [6].

In addition to intrusion detection, AIS have been deployed to detect viruses and worms [7]. Kephart deployed integrity monitors (based loosely on a minimalist AIS system) along with activity monitors to detect a variety of known viruses and worms. Forrest and colleagues have used AIS systems to detect changes in system executables using a similar approach [8]. Any change to system files is detected by exposing a set of antibodies to the typical suite of executables located on the computer system. Any change in the executable that would alter the contents of the programme would be flagged as an attack and appropriate action would be taken to preserve the integrity of the file system.

4.2 Fault Detection

This is used to detect malfunctions in a network or in a single system. The Negative Selection Algorithm is common here too. Bradley and Tyrell [9] created a hardware immune system that runs in real time to monitor continuously a machine for errors. They used the Negative Selection Algorithm to differentiate between normal and abnormal system operations. This system provides a unique solution to autonomous monitoring the state of a physical plant. The plant is examined and a feature set is extracted which depicts parameters and their values that are indicative of tolerated operation levels. If the parameter values fall outside of the expected operational range, an immune response is generated which signals an alert to the system monitor.

4.3 Data Mining

Data mining is the process of searching large volumes of data automatically for patterns using tools such as clustering or rule mining. J.Timmis and T.Knight [10] came up with an immunological approach to data mining which uses the clonal selection and called their Algorithm AINE (Artificial Immune Network). AINE uses a network of B-cells. AINE has been used in a variety of machine learning and pattern recognition tasks, typically in a hybrid approach. Tasks such as automated image analysis, spectra recognition, and function optimisation generally have all been met with varying degrees of success using AIS alone or in conjunction with other machine learning approaches (the AINE is such a hybrid approach).

5 Conclusion

This brief survey of the components of an AIS demonstrate that it has all of the hallmarks of a computational framework that is capable of an adaptive response to a

variety of novel stimuli. It provides this capability without any prior learning - the system is designed *de novo* to respond differentially to self and non-self. In the context of biometrics, the self is the authorised person and the non-self is everyone else. The ability to make this discrimination without being trained for both cases is a distinct advantage the AIS approach has over more traditional approaches such as supervised neural networks. Further, the basis of the immune system is very consistent – and would leave one to believe that this approach is a natural one for biometrics – in more ways than one! This paper describes essential features of the human artificial immune system and some notion of how the biological metaphor is naturally suitable for use in a variety of computer security applications. To date, virtually all research efforts in AIS in the context of computer security have focused on their deployment as an automated intrusion detection system. The authors believe that this is just the beginning – that AIS can be deployed in more classical biometrics such as keystroke dynamics, signature verification – essentially any form of biometrics would serve as a useful application domain. This is the basis of our future work in this field.

References

1. Forrest, S., Perelson, A.S., Allen, L., Cherukuri, R.: Self-nonself discrimination in a computer. In: SP 1994: Proceedings of the 1994 IEEE Symposium on Security and Privacy, pp. 202–212. IEEE Computer Society, Washington, DC (1994)
2. Ebner, M.m, Breunig, H-G., Albert, J.: On the use of negative selection in an artificial immune system. In: GECCO 2002 Proceedings of the Genetic and Evolutionary Computation, pp. 957–964. Morgan Kaufmann (2002)
3. Hofmeyr, S.A., Forrest, S.: Architecture for an artificial immune system. Evolutionary Computation 7(1), 45–68 (2000)
4. Wang, L., Jiao, L.: The immune genetic algorithm and its convergence. In: Fourth International Signal Processing Proceedings, pp. 1347–1350 (1998)
5. Chun, J., Kim, M., Jung, H., Hong, S.: Shape optimization of electromagnetic devices using immune algorithm. IEEE Transactions on Magnetics 33(2), 1876–1879 (1997)
6. Kim, J., Bentley, P.J., Aickelin, U., Greensmith, J., Tedesco, G., Twycross, J.: Immune System Approaches to Intrusion Detection – A Review. In: Nicosia, G., Cutello, V., Bentley, P.J., Timmis, J. (eds.) ICARIS 2004. LNCS, vol. 3239, pp. 316–329. Springer, Heidelberg (2004)
7. Kephart, J.O.: A biologically inspired immune system for computers. In: Brooks, R.A., Maes, P. (eds.) Artificial Life IV: Proc. of the 4th Int. Workshop on the Synthesis and Simulation of Living Systems, pp. 130–139. MIT Press
8. Hofmeyr, S.A., Forrest, S.: Immunity by design: an artificial immune system. In: Proc. of the Genetic and Evolutionary Computation Conference, pp. 1289–1296. Morgan Kaufmann
9. Bradley, D., Tyrrell, A.: A hardware immune system for benchmark state machine error detection. In: Proceedings of the 2002 Congress on Evolutionary Computing, vol. 1, pp. 813–818 (2002)
10. Knight, T., Timmis, J.: Aine: An immunological approach to data mining. In: ICDM 2001: Proceedings of the 2001 IEEE International Conference on Data Mining, pp. 297–304. IEEE Computer Society, Washington, DC (2001)