R&D

Artificial Immune Systems (AIS) : An Introduction

Would it be amazing if our computers could strike back after being invaded by viruses? Would it be brilliant if our internet system could detect an illegal intrusion before it intrudes the whole system? Kurt Kleiner in his article in the New Scientist [5], put it even better: "When one computer in cyberspace sneezes, software around the world can catch a cold. So is it time to provide computer networks with immune systems that kill viruses?". His question sparks a glimpse of the striking similarities between a network of computers and a living organism (after all, computer viruses are forms of artificial life). The remarkable and uniqueness of human immune system has always been an inspiration for most researchers to further explore our biological immune system, and Artificial Immune Systems (AIS) has been the result of this exploration. There have been number of works attempting at building AIS in various fields of study, such as virus detection, computer security and hardware fault tolerance system [3]. As engineering and computing problems grow ever more complex, alternative sources of inspiration for solutions to these problems are being sought by computer scientists and engineers. This article will reveal more on the concept behind AIS, its general frameworks, its applications and finally its potential for future development.

Similar to the biological immune system, which develops antibodies to detect and disable foreign organism or viruses found in the body, AIS basically works the same way by developing an antivirus to detect and disarm foreign entities or viruses. Theoretically, AIS can be defined as metaphorical computational systems developed using ideas, theories, and components, extracted from the immune system [3]. It is a relatively new field that tries to exploit the mechanisms present in the biological immune system in order to solve computational problems [4]. The foundation for AIS relies basically on its antibody-antigen (self and non-self) matching process for pattern recognition inside the human immune system. The concept of antibody-antigen matching has been the basis for the recognition and selective elimination mechanism that allows identification of foreign elements [4]. Basically, antigen and antibodies are represented as strings of data and the matching of these two strings is determined by a function that produces a binary output (match or not-match) [4]. Most of the AIS models have adopted these recognition processes in many ways such as the negative selection, clonal selection and the immune network theory. The following paragraph provides a brief description on each of the three immune models mentioned; negative selection, clonal selection and the immune network theory.

The negative selection deals with the immune system's ability to detect unknown antigens while not reacting to the self cells [1]. It contains three phases: defining self, generating detectors and monitoring the occurrence of anomalies. The concept is to generate a set of binary detectors by first randomly making candidates and then removing those that recognize or match the training self data [1]. These binary detectors can later be used to detect anomaly. Complementary to the role of negative selection, clonal selection is the theory used to explain the features of an immune response to an antigenic stimulus. It establishes the idea that only those cells that recognize the antigen proliferate, thus being selected against those that do not [1]. Different from the clonal selection which monitors the changes and responses in immune system only during the present of antigenic, immune network theory suggests that the immune system presents a dynamic behavior even in the absence of foreign antigen. It is suggested that the immune cells and molecules are capable of recognizing each other, what endows the system with an eigen-behavior that is not dependent on foreign stimulation [3].

The primary issue to be taken into account in the development of AIS is related to the kind of problem for AIS to be applied. Although the main roles of the immune system are to perform pattern recognition and to eliminate non-self or malfunctioning cells, it has great potential to be applied to diverse domain areas. Therefore, independently of the application domain, the first step in the modeling and simulation of most biological phenomena is to devise the models for the components or a framework of the system. The framework can be defined as a layered approach as illustrated in Figure 1 (taken from [2]). The basis for AIS is the application domain. For this domain, the way in which the components of the system will be presented has to be considered. Once a suitable representation is decided, one or more affinity measures are used to quantify the interactions of the elements of the system. The next layer involves the use of algorithms or processes to govern the behavior of the system. This then produces an engineered solution.

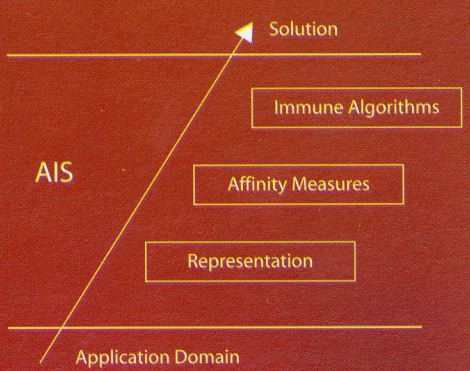

Figure 1: Layered Framework for AIS.

With the growing interest for AIS, future development will be possible in numerous applications such as in fault and anomaly detection, computer and network security. Long term research projects have been established in order to build a computer immune system which could supplement a simple computer security system with much more.

Host based intrusion detection methods construct a database that catalogues the normal behavior over time in terms of the system calls made etc. The database monitors for any system calls not found in the normal behavior database. This approach is computationally inexpensive and can be applied in real time. In addition, it also has the advantage of being platform and software independent. An alternative method is the network based intrusion detection approach. This deals with the issue of protecting networks of computers rather than an individual computer. This is achieved in a similar way in monitoring network services, traffic and user behavior and attempts to detect misuse or intrusion by observing departures from normal behavior. Attempts also have been made to apply the immune network idea to control large populations of robots to have some form of self-organizing group behavior. Work by Singh and Thayer [1] attempts to create a group of robots, which self-organize to search for food without any global control mechanism. Apart from that, the pattern recognition task performed by the immune system is much in common with the aerial image segmentation problem. Negative selection algorithm is used to construct a set of detectors capable of recognizing everything but the desired class.

AIS emerged as a new computational paradigm in AI. It is being used in many applications such as anomaly detection, pattern recognition, data mining, computer security, adaptive control and fault detection [1]. During the last five years, AIS has earned its position on the map of soft computing paradigm. Despite the initial success of AIS techniques, there remain many open issues. As the field is relatively new, most of the existing works have been exploratory, and the algorithms do not scale. The following are some aspects that need to be dealt with in order to make AIS as useful problem solving technique in future [1]:

- Improvement of the efficiency of the algorithms.
- Enhancement of the representation.
- Introduction of other mechanisms as necessary.
- Development of a unified architecture that can integrate several AIS models.

In conclusion, the immune system is a remarkable natural defense mechanism. It exhibits capabilities such as learning, memory, and adaptation. For these reasons, and many others, the immune system can be viewed as a mechanism of vast potential for inspiration in a variety of domains. By utilizing the basic concepts of the immune system it is possible to construct artificial immune systems that can be applied to numerous computational scenarios.

References

[1] Dasgupta, D., Ji, Z., and Gonzales, F. (2003), "Artificial Immune System (AIS) Research in the Last Five Years", *Proc. of the ICEC'03*, pp. 123-130.

[2] de Castro, L. N., and Timmis, J. (2002), "Artificial Immune Systems: A New Computational Intelligence Approach", Springer, UK.

[3] de Castro, L. N., and Timmis, J. (2002), "Artificial Immune Systems: A Novel Paradigm to Pattern Recognition", *Proc. of the ICARIS'02*, pp. 67-84.

[4] Gonzales, F., Dasgupta, D., and Gomez, J. (2003), "The Effect of Binary Matching Rules in Negative Selection", *Proc. of the GECCO'03*, pp. 195-206.

[5] Kleiner, K. (1997), "The Internet Strikes Back", *New Scientist*, pp. 35.

Prepared By :
Hasnah Ahmad
School of Computer & Communication Engineering
Kolej Universiti Kejuruteraan Utara Malaysia
hasnahahmad@kukum.edu.my