# Applications of Aritificial Immune Systems

**Suhair H. Amer, Ph.D.**
Department of Computer Science, Southeast Missouri State University, Cape Girardeau, MO, USA

**Abstract—***In recent decades, Artificial Immune Systems (AISs) have appeared as an approach dealing with security systems and classification problems. This paper briefly surveys AIS basic concepts, features and principles, approaches and applications.*

**Keywords***:* Artificial Immune Systems, applications of AIS, biologically inspired systems

## 1 Introduction

An Artificial Immune System (AIS) is a biologically inspired computing which is currently investigated to solve many problems. Such a method was inspired by the Human Immune System (HIS) that can detect and defend against harmful and previously unseen invaders. AISs have been built for a wide range of application domains including document classification, fraud detection, and network- and host-based intrusion detection. Section 2 will discuss the basic concepts used to build an AIS. Section 3 will discuss AISs features and principles that distinguish them from other methods. Section 4 discusses the philosophies or approaches of applying immune system concepts. Section 5 discusses examples of applications of AISs. Finally, section 6 concludes the paper.

## 2 Artificial Immune systems Basic Concepts

To implement a basic AIS, four decisions have to be made: encoding, similarity measure, selection and mutation.

### 2.1 Initialization and Encoding

It is very important to choose a suitable encoding [1] to insure the algorithm's success. The antigen and antibody should be defined in the context of an application domain. For example, antigens can represent intrusion data instances, and antibodies bind to antigens identifying an intrusion.

### 2.2 Similarity or Affinity Measure

A good matching algorithm guarantees that the AIS works properly. The primary response in the immune system [2] uses learning mechanism to identify antigens that have not been detected by a detector before. When a B cell is activated after binding to a pathogen, it starts cloning itself and the cloned cells then undergoes a somatic hyper mutation to create child B cells with mutated receptors. Then all B cells compete with each other.

### 2.3 Negative Selection

In the negative selection algorithm [1], a set of trusted behavior describing self is defined. During the initialization of the algorithm, a large number of detectors are created. Then these detectors are subjected to a matching algorithm that compares them to self behavior. Any matching detector will be eliminated and those that do not match are selected which explains the term negative selection.

### 2.4 Somatic Hyper mutation

Somatic hyper mutation [1] is an optional process associated with negative selection. Rather than ignoring matching detectors in the first phase of the algorithm, they can be mutated to save time and effort. Also, depending on the degree of matching, the mutation could be more or less strong.

### 2.5 Cross-Reactivity and Associate Memories

When a B-cell encounters subsequent antigens it responds quicker (secondary response) in which the memory cells for an earlier antigen quickly start producing large quantities of a specific antibody. In general, B-cell receptors do not require an exact match to an antigen to be activated. Therefore, some memory cells can react to new antigens producing a secondary response which is termed, the cross-reactive memory [3].

## 3 AIS Features and Principles

In general AISs have the following desirable features and principles [4]:

- Distributed: the presence of an infection is determined locally with no central coordination taking place.

- Scalability: communication and interaction between components are localized and there is little

overhead associated when the number of components is increased.

- Multi-layered: security is achieved by combining multiple layers of different mechanisms to provide high overall security.

- Diversity: it is less likely that the security vulnerabilities in one system be widespread.

- Robustness: No single component or cell of the human immune system is essential and can be replaced.

- Autonomy: no outside management or maintenance is required as classification and elimination of pathogens and repairing self is done locally.

- Adaptability: The immune system learns to detect new pathogens, and retains the ability to recognize previously seen pathogens through immune memory.

- No secure layer: Any cell in the human body can be attacked by a pathogen or even another immune system cell.

- Dynamically changing coverage: since the immune system cannot maintain a set of detectors large enough to cover the space of all pathogens, it maintains a random sample of its detector repertoire circulating throughout the body.

- Identity via behavior: identity is verified through the presentation of peptides, or protein fragments.

- Anomaly detection: ability to detect pathogens that has never been encountered before.

- Flexibility or Imperfect detection: By accepting imperfect detection, the immune system increases the flexibility with which it can allocate resources.

- Detector replication: The human immune system replicates detectors to deal with replicating pathogens.

- Memory : the immune system reacts more rapidly the second time against pathogens that are similar to the ones that were encountered previously.

- Implicit policy specification: definition of self in the immune system is empirically defined by monitoring proteins that are currently in the body.

# 4 Immune System Approaches

Application of immune system concepts can be based on the following distinct philosophies [5]:

## 4.1 Negative Selection (NS)

Negative selection concepts are concerned with eliminating immature cells that bind to self antigens. This allows the HIS to detect non-self antigens without mistakenly detecting self-antigens.

## 4.2 Danger Theory

The Danger Theory describes which data should be represented. It focuses on the presence of dangerous signals and goes beyond and overcomes many of the limitations of self–non-self selection [1].

## 4.3 Immune Network Theory

The hypothesis of the immune network theory states that the immune system maintains an idiotypic network of interconnected B-cells for antigen recognition. These cells both stimulate and suppress each other in certain ways that lead to the stabilization of the network. For example, two B-cells connect if their shared affinities exceed a certain threshold, and the strength of the connection is directly proportional to the affinity they share [1].

## 4.4 Clonal Selection Principle

Clonal Selection Principle [1] describes the basic features of an immune response to an antigenic stimulus. Only the cells that recognize the antigen proliferate and are selected against those that do not.

## 4.5 Idiotypic Networks

The Idiotypic network hypothesis [1] builds on the recognition that antibodies can match other antibodies as well as antigens. This could be used to explain how the memory of past infections is maintained and could result in the suppression of similar antibodies. In general, the nature of an Idiotypic interaction can be either positive or negative.

## 4.6 Other methods

Although negative selection and the danger theory are the most popular approaches in AIS for intrusion detection, some researchers choose to create AIS based on alternative ideas. For example, Forrest et. al [6] build an intrusion detection system (IDS) based on an explicit notion of self within a computer system. The system was host-based, examining specifically privileged processes. The system collected self-information to construct a database of normal commands.

# 5 Artificial Immune systems Applications

This section briefly introduces some application areas where AIS have been applied.

## 5.1 Recommender Systems

Collaborative filtering (CF) [7][8] is one of the common applications of AIS. CF is the term for a broad range of algorithms that use similarity measures to obtain recommendations. In general, any problem domain where users are required to rate items is amenable to CF techniques. For example, commercial applications are called recommender such as movie recommendation. Traditionally, recommended items are treated as black boxes and recommendations are based purely on the votes of neighbors, and not on the content of the item. A user profile which consists of the preferences of a user that is usually a set of the user's votes on an item. These profiles are then compared to build a neighborhood.

Morrison and Aickelin [9] applied idiotypic network theory to build their web site recommender AIS based system. The idiotypic network theory states that interaction in the immune system do not only occur between antibodies and antigens but also between antibodies and each other. Therefore, the antibody may be matched by other antibodies. This activation can spread throughout the population. In general, the interaction may have a positive or a negative effect on a particular antibody-producing cell. Morrison and Aickelin idea is that antibodies that are very similar to each other had their concentrations reduced. This allowed the creation of a set of users that are similar to a user but quite still different to each other which enhances the recommendation accuracy of the system.

Hsieh et. al [10] employed AIS to deal with classification problem. In their paper, an AIS algorithm is developed and applied to a two-group classification problem. They discuss a Taiwanese banking industry example and the financial ratios of each bank from 1998 to 2002 were collected. Their system had a 10% better performance than the three soft computing early warning systems (GNN, CBR and BPN). Their AIS outperforms the statistical early warning systems (LR and QDA) at least 24%.

Singh and Nair [11] outline a robot controller based on a combination of the innate and adaptive immune systems. The learner robot learns to accurately follow a track. It can sense when it is on the track and when it loses it. If it loses the track, it first tries to find it on its own and then requests the assistance of a helper robot, who will guide it back to the track. The general idea is to have the learner robot learn to navigate weak portions of the track autonomously, without losing the track and having to be guided back by the helper. The proposed immune system has two type of response governed by separate innate and adaptive subsystems.

Burgess has developed Cfengine [12], an autonomous agent and a middle-to-high level policy language for building expert systems to administrate and configure large computer networks. The system adapts the danger model using autonomous and distributed feedback and healing mechanism triggered when a small amount of damage is detected. Cfengine automatically configures large numbers of systems on a heterogeneous network with an arbitrary degree of variety in the configuration.

## 5.2 Security based systems

Security systems may include virus detection and intrusion detection systems. Virus detection is viewed as a self-non-self discrimination problem. Targets such as legal user activities, legal application usage activities, and uncorrupted data are monitored as self and the AIS are expected to discriminate them from illegal user activities, illegal application usage activities, and virus infected data.

The Computer Virus Immune System (CVIS) approach [13] is able to perform virus analysis, repair infected files and propagate the analysis results to other local systems. In addition, CVIS was designed to operate under a distributed environment using autonomous agents. The system was tested against the TIMID virus, which infects .com files within a local directory. The test reports showed the sensitivity of detection and error results on different matching thresholds. It showed a detection rate of up to 89% but had a very high scalability problem since it required approximately 1.05 years for generated antibodies to scan an 8GB hard disk drive. However, novel concepts such as life span, activation threshold and co-stimulation were investigated.

Sarafijanovic and Le Boudec [14] built an immune-based system to detect misbehaving nodes in a mobile ad-hoc network. The authors considered a node to be functioning correctly if it adhered to the rules laid down by the Dynamic Source Routing (DSR) protocol. Each node in the network monitored its neighboring nodes and collected one trace per monitored neighbor. Four events were sampled over fixed and discrete time intervals to create a series of data sets. This created a binary antigenic representation.

Stillerman et. al [15] introduced an immunity-based intrusion detection approach that was particularly applicable to Common Object Request Broker Architecture (CORBA) applications. CORBA is a popular common messaging middle-ware that enables the communication of distributed objects for distributed applications. The authors employed the same approach reported in [16] to detect a misuse

attacks performed by a legal user of the system. The results showed that the system was able to detect anomalies without high false positive error rates.

Dasgupta [17] provided the conceptual view and a general framework of a multi-agent anomaly based intrusion detection system and response in networked computers. The immunity based agents in the system roamed around nodes and monitored network situation. Each agent can recognize other activities and can take appropriate actions according to its predefined security policies. The agent can adapt to its environment dynamically and can detect novel and known attacks. Network activities were monitored on the user, system, process and packet levels.

Pagnoni and Visconti's [18] NAIS IDS is inspired by innate immune mechanisms. Their immune system is a multilayer defense system. The innate immune system is the first line of defense which is able to recognize self quickly. Their system compiles a list of all observed process names during a training period containing only normal usage. A set of "digital macrophages" is then created which monitors the system and generates an alert when any previously unseen process name is observed.

# 6 Conclusion

The human immune system has been successful in defending different human organs against a wide range of harmful attacks. Negative selection and Danger Theory are two of the commonly used philosophies in building artificially immune based systems. In general, to implement a basic artificial immune system, four decisions have to be made: encoding, similarity measure, selection and mutation. This paper briefly discussed the features and principles that make AIS desirable for building applications dealing with security and recommender systems.

# 7 References


[1] U. Aickelin and D. Dasgupta. Artificial Immune Systems Tutorial. To appear in Introductory Tutorials in Optimization, Decision Support and Search Methodology (eds. E. Burke and G. Kendall), Kluwer. 2005.

[2] Stephanie Forrest and Steven A. Hofmeyr. Immunology as information processing, In Design Principles for the Immune System and Other Distributed Autonomous Systems, edited by L.A. Segel and I. Cohen. Santa Fe Institute Studies in the Sciences of Complexity. New York: Oxford University Press. (2001).

[3] S. Forrest, S. Hofmeyr. Engineering an Immune System. Graft, Vol. 4, No. 5, 2001, 5-9

[4] A. Somayaji. Operating System Stability and Security through Process Homeostasis. PhD thesis, University Of New Mexico, 2002.

[5] J. Kim, P. Bentley, U. Aickelin, J. Greensmith, G. Tedesco and J. Twycross. Immune System Approaches to Intrusion Detection - A Review. Natural Computing, Springer, in print, pp XXX. 2007.

[6] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff. A sense of self for Unix processes. In Proceedings of 1996 IEEE Symposium on Computer Security and Privacy, pp. 120-128 (1996).

[7] S. Cayzer and U. Aickelin. A Recommender System based on the Immune Network. Proceedings CEC, pp 807-813. 2002.

[8] D. L. Chao and S. Forrest. Information Immune Systems. In Proceedings of the First International Conference on Artificial Immune Systems (ICARIS), pp. 132-140 2002.

[9] T. Morriso and U. Aickelin. An AIS as a Recommender System for Web Sites. 1st International Conference on AIS, pp 161-169. 2002.

[10] Jih-Chang Hsieh, Shih-Hsin Chen and Pei-Chann Chang. Application of Artificial Immune System in Constructing a Financial Early Warning System: An Example of Taiwanese Banking Industry. Proceeding ICICIC '07. Proceedings of the Second International Conference on Innovative Computing, Information and Control. IEEE Computer Society Washington, DC 2007.

[11] C. T. Singh and S. B. Nair. An Artificial Immune System for a Multi Agent Robotics System. In Proc. of the 4th World Enformatika International Conference on Automation Robotics and Autonomous Systems (ARAS 2005), pages 308–311, 2005.

[12] M. Burgess. Evaluating cfegine's immunity model of site maintenance. In Proceeding of the 2nd SANE System Administration Conference (USENIX/NLUUG), 2000.

[13] P. K. Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont. An artificial immune system architecture for computer security applications. IEEE Transactions on Evolutionary Computation, 6(3):252-280, June 2002.

[14] S. Sarafijanovic and J.-Y. Le Boudec. An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile Ad-Hoc

Networks. IEEE Transactions on Neural Networks, Special Issue on Adaptive Learning Systems in Communication Networks, 16(5):1076–1087, 2005.

[15] M. Stillerman, C. Marceau, and M. Stillman. Intrusion detection for distributed application. Communications of the ACM, 42(7):62-69, July 1999.

[16] S. A. Hofmeyr, S. Forrest and A. Somayaji. Intrusion detection using sequences of system calls. Journal of Computer Security, 6 (1998), 151--180.

[17] D. Dasgupta. Immunity-based intrusion detection systems: A general framework. In Proc. of the 22nd National Information Systems Security Conference (NISSC), October 1999.

[18] A. Pagnoni and A. Visconti. An innate immune system for the protection of computer networks. In Proc. of the 4th International Symposium on Information and Communication Technologies, pages 63–68. Trinity College Dublin, 2005.