Chapter 1. Introduction

1.1 Motivation

With the development of communication networks, the Internet has become critical infrastructure to a modern society. The explosive growth of Internet users has motivated the rapid expansion of electronic commerce and other online-based services. Behind convenience and efficiency resulted from these services, there lies a dark side: vulnerability to cyber threats. A current society that depends on network technology ever more than before is exposed to probably one of the most threatening attacks. In the last year, even security conscious e-commerce companies like Amazon.com, e-Bay and CNN.com were hacked by intruders [silicon, 2000]. These recent attacks have encouraged the U.K. government to provide £15 billion to combat Internet attack in 2000 [Dti-mi, 2000]. Likewise, increasing importance of computer security motivates various angles of security related research that provide new solutions, which might not be achievable by more conventional security approaches.

The key attributes of rigorous computer security are confidentiality, integrity and availability [Bernstein *et al.*, 1996]. The prevailing approach to the fulfilment of these requirements is intrusion prevention. Intrusion prevention is an attempt to build a completely secure computer system, by determining and eliminating various security vulnerabilities. Alongside this approach, intrusion detection is another significant method used to secure systems. The main goal of intrusion detection is to detect unauthorised use, misuse and abuse of computer systems by both system insiders and external intruders.

There are various approaches to building intrusion detection systems (IDS's). They mainly employ two techniques: *anomaly detection* and *misuse detection* [Lunt, 1993; Sundaram, 1996; Axelsson, 2000]. The anomaly detection approach establishes the profiles of normal activities of users, systems or system resources, network traffic and services using the audit trails generated by a host operating system or a network-scanning program. This approach detects intrusions by identifying significant deviations from the normal behaviour patterns of profiles. The misuse detection approach defines suspicious misuse signatures based on known system vulnerabilities and a security policy. This approach probes whether these misuse signatures are present or not in the auditing trails.

The strength of the anomaly detection approach is that prior knowledge of the security flaws of the target systems is not required. Thus, it is able to detect not only known intrusions but also unknown intrusions. In addition, this approach can detect the intrusions that are achieved by the abuse of legitimate users or masqueraders without breaking security policy [Denning, 1987; Porras, 1992]. However, it has several limitations, such as high false positive detection error, the difficulty of handling gradual misbehaviour and expensive computation [Porras 1992; Lunt *et al.*, 1992; Mykerjee *et al.*, 1994]. In contrast, the misuse detection approach detects only previously known intrusion signatures. The advantage of this approach is that it rarely fails to detect previously notified intrusions [Denning, 1987; Ilgun *et al.*, 1995] However, this approach cannot detect new intrusions that have never previously been monitored. Furthermore, this approach is known to have other drawbacks such as the inflexibility of misuse signature rules and the difficulty of creating and updating intrusion signature rules [Porras 1992; Ilgun *et al*., 1995; Kumar, 1995]. These strengths and limitations of the two approaches imply that an effective IDS should employ an anomaly detector and a misuse detector in parallel [Mykerjee *et al.*, 1994]. However, most available commercial IDS's use only misuse detection because most developed anomaly detectors still cannot overcome the limitations described above[1]. This trend motivates many research efforts to build effective anomaly detectors for the purpose of intrusion detection.

Human immune systems have been successful at protecting the human body against a vast variety of foreign pathogens or organisms. One most interesting feature of the human immune system is the discriminative power to detect harmful pathogens without attacking human body self cells. The human immune system distinguishes previously known and unknown pathogens from human body self cells via its own evolutionary mechanism, which is similar to evolution of organisms in nature. The human immune system has a multi-layered architecture [Forrest *et al.*, 1997; Tizard, 1995]. It consists of passive layers such as the skin, mucus membranes, *pH*, temperature and generalised inflammatory responses, and adaptive layers including both the humoral (B cell) and cellular (T cell) mechanisms. The passive layers are called natural immune systems and the adaptive layers are called adaptive immune systems [Paul, 1993].

The natural immune systems are innate and ever present, while the adaptive immune systems are dynamically generated against the non-self organisms encountered during their lifetimes [Paul, 1993; Tizard, 1995; Playfair, 1996]. The non-self organisms that intrude into the human body, such as bacteria and viruses, are rapidly detected and eliminated by natural immune systems. These immune responses are non-specific in their effects and thus they are effective against a diverse but relatively common group of antigens at the same time. The adaptive immune systems cope with the foreign organisms that do not attack human body often or have never attacked before, and thus evade the natural immune systems. In addition, when the adaptive immune systems detect the unusual attackers, they remember these unusual attackers and are able to detect them in the future. While natural immune systems are unaltered on repeated infection and provide the radical mechanisms to detect and eliminate infected organisms, adaptive immune systems provide more efficient mechanisms that are adaptively changed and remember infections.

The overall natural and adaptive immune system is implemented through the interactions between a large number of different types of innate and acquired cells rather than the function of one particular human organism. Each cell involved in immunity performs a different job in

[1] There are a number of anomaly detector prototypes developed in various research labs.

order to complete overall immune process. For example, natural immune systems usually handle viruses and bacteria via the interaction between chemicals such as complements, interferon and white blood cells such as macrophages. Complements activate the production of inflammatory effects, interferon block the replication of virus and macrophages remove damaged tissues and cells. This co-operation between millions of different cells implies that the human immune system is distributed.

The above summary leads to an analogy between human immune systems and intrusion detection systems. The natural immune system is akin to the misuse detector of IDS and the adaptive immune system is similar to the anomaly detector of IDS. Both natural immune systems and misuse detectors have the prior knowledge of attackers and detect attackers based on this knowledge. Similarly, both adaptive immune systems and anomaly detectors adaptively generate new detectors to detect previously unknown attackers. With respect to the research on IDS's, this anomaly-detector-like feature of the adaptive immune system attracted a growing number of computer scientists and they have proposed several different computer immune models [Dasgupta, 1998a; De Castro and Von Zuben, 2000a].

These models are still at an early stage and not many models have been applied to solve real world problems. It has not been proved whether the artificial immune model is able to show performance as significant as other biologically inspired AI techniques such as neural networks and genetic algorithms. Particularly, most approaches to build an artificial immune system (AIS) have been attempted mainly by implementing only a small subset of overall human immune mechanisms [Dasgupta, 1998a]. This is because the nature of human immune systems is very complicated and sophisticated and thus it is very difficult to implement perfect human immune processes on a computer. However, as seen from other immunology literature [Paul, 1993; Tizard, 1995], an overall immune reaction is the carefully co-ordinated result of numerous components such as cells, chemical signals, enzyme, etc. Therefore, the omission of crucial components in order to make the development of AIS simpler and more applicable may detrimentally affect the performance of an AIS. This implies that improved artificial immune responses can be expected if the roles of crucial components of human immune systems are correctly understood and they are implemented in the right way.

1.2 Thesis Hypothesis

The main hypothesis of this research can be defined as follows:

*The **combination** or **integration** of separate artificial immune algorithms into one system is **effective** in **detecting intrusions**.*

This research aims to improve the effectiveness of currently available artificial immune systems by integrating them. The effectiveness of an integrated new system is measured by how much the new system satisfies the requirements of intrusion detection systems. In order to show the validity of the above research hypothesis, individual research areas that can address sub-answers of the research hypothesis are identified. These areas are presented as thesis goals in the next section.

1.3 Thesis Goals

There are five main goals of this thesis:

1. **Identify the components of the human immune system that are crucial to the improvement of AIS for the application such as intrusion detection.**
   Prior to proposing a new integrated artificial immune model, it is essential to comprehend as much as possible about how human immune systems work. This understanding is required in order to identify components of human immune systems providing their salient features, that are pivotal for the development of a more effective IDS.

2. **Propose an integrated new artificial immune model**
   Based on new understanding of crucial components of human immune systems, a new artificial immune model should be proposed that embeds useful components into one system.

3. **Identify limitations of current AIS that are popularly used for intrusion detection**
   In order to show the benefits of an integrated new artificial immune model as IDS, the limits of individual artificial immune algorithms should be identified.

4. **Understand the role of each different artificial immune algorithm as a single component of an integrated system.**
   In order to verify the previous identification of crucial immune components, each component of a new artificial immune model should be examined in terms of whether it provides beneficial immune features required by the IDS.

5. **Study new effects and limitations of an integrated model**
   Finally, based on the comprehension of individual components within the integrated artificial immune model, new benefits and limitations of the new model as an IDS should be analysed.

1.4 Thesis Contributions

This thesis makes the following specific contributions.

1. The components of human immune systems that are crucial to the improvement of artificial immune systems for intrusion detection are identified (chapter 3).

2. A systematic framework for artificial immune systems for network intrusion detection is introduced by combining three evolutionary stages: negative selection, clonal selection and gene library maintenance. It is demonstrated that this framework can fulfil the role of a network-based intrusion detection system (chapter 3).

3. It is demonstrated that the negative selection algorithm used in this thesis has a severe scaling problem when applied in a real network environment (chapter 4).

4. It is demonstrated that a static clonal selection algorithm with a negative selection operator achieves efficient niche maintenance and acceptable self-tolerance (chapter 5).

5. A dynamic clonal selection algorithm that combines three evolutionary stages allows the AIS to be adaptable to dynamically changing antigen behaviours (chapter 6).

6. The effect of three parameters on the behaviour of the dynamic clonal selection algorithm is analysed. These parameters are: tolerisation period, activation threshold and life span. Satisfactory TP and FP rates are obtained by setting these parameters to appropriate values. (chapter 6).

7. The extension of the dynamic clonal selection algorithm to employ deletion of memory detectors reduces high FP rates observed when previously observed normal behaviours no longer represent normal behaviours (chapter 7).

8. It is demonstrated that simulation of gene library evolution using hypermutation reduces the amount of human intervention (chapter 7).

9. The integrated artificial immune model for intrusion detection is assessed in terms of the five research goals presented in this chapter (chapter 8).

1.5 Thesis Structure

Following this chapter, this thesis presents the studies performed to satisfy the five main research goals over the next seven chapters.

Chapter 2 presents a review of existing literature related with two fields: intrusion detection systems and immune systems. The definition of intrusion detection and the taxonomy of existing intrusion detection systems are introduced. IDS categories including anomaly detection systems and network-based systems, which are especially analogous to the human immune model, are presented. The second part of this chapter provides a wide review of literature related with the human immune system and artificial immune systems. An overview of how the human immune system works is outlined. The introduction of available artificial immune algorithms and systems follows this outline. The introduced artificial immune algorithms and systems are described in terms of their theoretical ideas and their applications.

Chapter 3 presents a novel artificial immune model for network intrusion detection, which can satisfy a set of general requirements for network-based IDS's. This is achieved by identifying the limitations of currently available network-based IDS's and several significant aspects of the human immune system that can contribute to develop effective network-based IDS's. This chapter also defines the research scope within the presented AIS model, which is studied in this thesis.

Chapter 4 investigates the feasibility of a negative selection algorithm on real network traffic data. An independent negative selection algorithm has been known as the most prevalent attempt that applies a human immune mechanism to network intrusion detection problems [Somayaji *et al.*, 1997]. The negative selection algorithm is implemented and applied on large amounts of network traffic data. In order to apply a negative selection algorithm in a real network environment, a broader but more realistic range of self-sets are defined and used in experiments. The results of the experiments showed a severe scaling problem for the negative selection algorithm. Such results direct this research to re-define the role of the negative selection algorithm within the overall artificial immune system framework.

Chapter 5 is devoted to the investigation of the use of a static clonal selection algorithm with a negative selection operator. This chapter investigates the use of the niching strategy provided by a static clonal selection algorithm within the presented AIS model. In order to avoid the scaling problem of negative selection, the AIS adopts a static clonal selection algorithm which embeds a negative selection operator within it. This component is especially developed for the purpose of building a misuse detector in a more efficient way. In order to let detectors evolve to be able to detect more complicated antigens, a number of modifications are made by adopting some techniques available in a concept learning research field. A series of experiments are performed for the purpose of analysing the effect of detector and antigen sample sizes on performance. In addition, experimental results are tested in terms of whether the embedded negative selection operator plays an important role in the AIS by helping it to maintain a low false positive rate.

Chapter 6 introduces a dynamic clonal selection algorithm that is equipped with two new properties: firstly to learn normal behaviours by undergoing only a small subset of self antigens at one time and secondly to replace detectors whenever previously observed normal behaviours no longer represent current normal behaviours. In order to obtain these features, this new algorithm adopts several new human immune features such as immature, mature and memory detectors, tolerisation period, activation threshold and life span. The effects of these new features are tested through two sets of experiments, which are performed for the purpose of analysing whether the new algorithm provides the two properties mentioned above.

Chapter 7 extends the dynamic clonal selection algorithm that is introduced in Chapter 6. The experimental results presented in Chapter 6 show that the dynamic clonal selection algorithm has difficulty in yielding the second property, which is updating detectors appropriately when previously learned normal behaviours are suddenly changed. The extended dynamic clonal selection algorithm employs memory detector deletion based on antigen detection results and gene library evolution using hypermutation. These two new mechanisms are evaluated to see if they allow the AIS to overcome the problem found in Chapter 6.

Chapter 8 reviews the research contributions made by this thesis. The review concentrates on whether these contributions fulfil the five research goals presented in this chapter. Finally, the thesis concludes with suggestions for future work.