

Appendix A. Detailed Description of The Human Immune System

A.1. Introduction

The human immune system has a multi-layered architecture [Forrest *et al.*, 1997; Playfair, 1996]. Conceptually, 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; Playfair, 1996; Tizard, 1995]. 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 the 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 organ. Each cell involved in immunity performs a different job in order to complete the overall immune process. For example, natural immune systems usually handle viruses and bacteria via the interaction between complements, interferon and other cells such as macrophage [Playfair, 1996]. Complements activate the production of inflammatory effects, interferon block the replication of virus and macrophage 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, the most formidable feature of human immune systems is its adaptive and distributed detection. Therefore, it is essential to understand adaptive immune systems more deeply. In this section, the adaptive immune systems are introduced and particularly the genetic mechanisms that facilitate these properties.

A.1.1 Specific Recognition

The adaptive immune system consists of various different types of cells and each plays an important role [Playfair, 1996; Forrest and Hofmeyr, 2001]. The central role is played by lymphocytes in showing specific antigen recognition (see, figure A.1). Each lymphocyte is specialised in reacting to a limited number of structurally related foreign cells, known as antigens. This is possible because each lymphocyte has a set of specific receptors on its surface and these receptors have a complementary shape to the specific determinants, known as epitopes, on the antigen surface. When these receptors match the epitopes of a specific antigen, which have complementary structures, this antigen is recognised. The millions of lymphocytes in a human body can react against millions of different types of antigens.

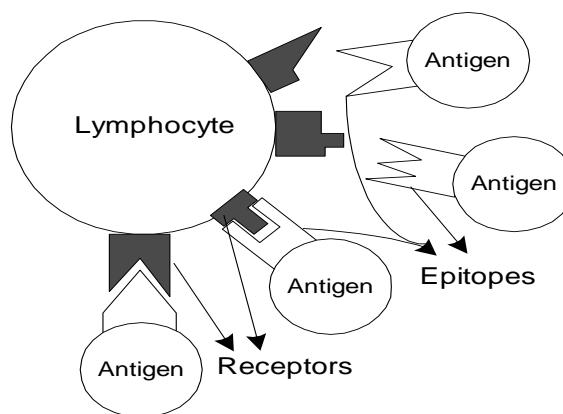


Figure A.1 Antigen Recognition by a lymphocyte

B-lymphocytes

Lymphocytes can be categorised into two main types according to their function: B-lymphocytes and T-lymphocytes [Playfair, 1996; Life, 1993; Forrest and Hofmeyr, 2001]. B-cells, which are short for B-lymphocytes, are the precursors of antibody-secreting cells. Antibodies are proteins and they play the role of the receptor of B-lymphocytes. The antibodies on B-cell surfaces bind to the antigens, leading to their removal. T-cells, which are also short for T-lymphocytes, do not secrete antibodies, but they have their own receptors binding to antigens. As mentioned above, the antibodies of B-cells have the specific shapes which are

complementary to the epitopes of antigen surfaces. A specific antigen is recognised by B-cells through a match between B-cell antibody receptors and antigen epitopes.

T-lymphocytes

T-cells are classified into two types: helper T-cells and killer T-cells. Helper T-cells show significant regulatory functions, such as the ability to help or suppress the development of specific types of immune responses, including the antibody production. On the other hand, killer T-cells kill virus infected cells. The details of activation of these cells are discussed in the section A.1.4.Activation. Moreover, T-cells have a significant antigen recognition procedure that is not preformed by B-cells. T-cells can detect antigens even when they are hidden inside human host cells. Among pathogens existing in the human body, some pathogens are called intracellular pathogens [Playfair, 1996; Tizard, 1995]. They live inside host cells and thus are not visible to B-cells. But, all cells in human body have Major Histocompatibility Complex (MHC) molecules on their surfaces and these MHC molecules collect fragments of proteins hiding inside the cell. When a self cell is infected by virus and this virus hides inside the self cell, MHC on the surface of the infected self cell contains a fragment of the virus protein. T cells recognise infected self cells by binding their receptors to MHC molecules. Therefore, T-cells can detect antigens even when they are hidden inside human host cells.

A.1.2 Genetic Structure of Lymphocytes

The receptors of antibodies are proteins and the proteins consist of chains of assorted amino acids linked by peptide bonds. The sequence of amino acids determines the different protein chains and the specific protein chains determine the binding shapes of antibodies. The specificity of an individual lymphocyte is determined by the arrangement of gene segments in DNA that instruct the sequence of amino acids [Life, 1993; Tizard, 1995]. In addition, B-cells and T-cells have their own unique DNA gene libraries. The unique genetic structures of B-cell antibody receptors and T-cell receptors are determined by rearranging genes selected from the gene libraries. Therefore, it is important to understand the gene structure and the gene libraries of receptors according to the different lymphocytes: B-cell and T-cell.

B-lymphocytes

The receptor of a B-cell is made up of a pair of heavy chains and a pair of light chains [Life, 1993; Paul, 1993]. Figure A.2 shows the structure of B-cell receptors. The connected heavy chains form a ‘Y’ shape with the light chains located on the upper parts, alongside the heavy chains. Each chain has a variable domain and a constant domain.

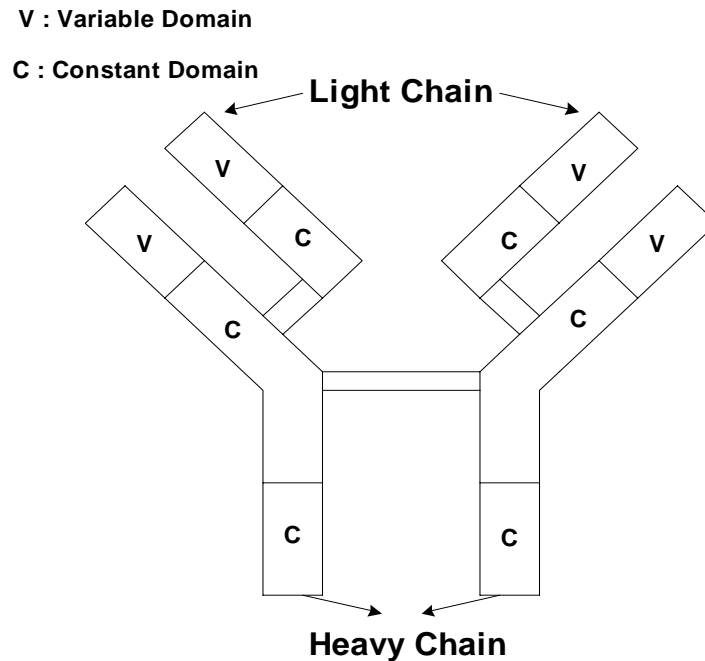


Figure A.2 B-cell receptor structure

The genes determining the receptor shape in the variable domain are highly variable from one to another and contribute to the binding of antigen. The genes constructing the receptor shape in the constant domain are constant from one to another and show various biological effects when the variable region of the antibody receptors binds to the epitopes of a specific antigen. The variable domain is made up of three different regions: variable (V), diversity (D) and joining (J). The variable domain of the heavy chain is made of all three regions (V-D-J) and the variable domain of the light chain is made of only two regions (V-J). The heavy chain shows more diverse gene combinations than the light chain by adding the diversity region. In contrast, the constant domain is comprised of one region: constant region (C). Each region is comprised of a number of gene segments selected from unique gene libraries: V, J, D, or C (see, figure A.3). For example, the V region gene library of heavy chain contains about 350 different genes and 100~300 genes are selected to make a V region of a heavy chain.

T-lymphocytes

There exist two types of T-cells based on the receptors on the cell surface [Life, 1993; Paul, 1993]. The majority of T-cells consist of α chains and β chains and a small group of T-cells consists of γ chains and δ chains. All of these four families contain V, J, and C regions and β and δ gene families additionally contain the D region in their variable domains. While B-cell receptor chains have only one constant region, T-cell receptors have two constant regions.

A.1.3 Development

The receptors of B-cells and T-cells should be able to bind a vast number of different shapes of antigen epitopes. If a specific receptor can bind a specific epitope, how can a limited number of antibodies detect all existing antigens? The maintenance of B-cell antibody and T-cell receptor diversity is achieved via sophisticated genetic mechanisms. As described above, B-cells and T-cells have their own gene libraries such as heavy, light, α , β , γ and δ chains.

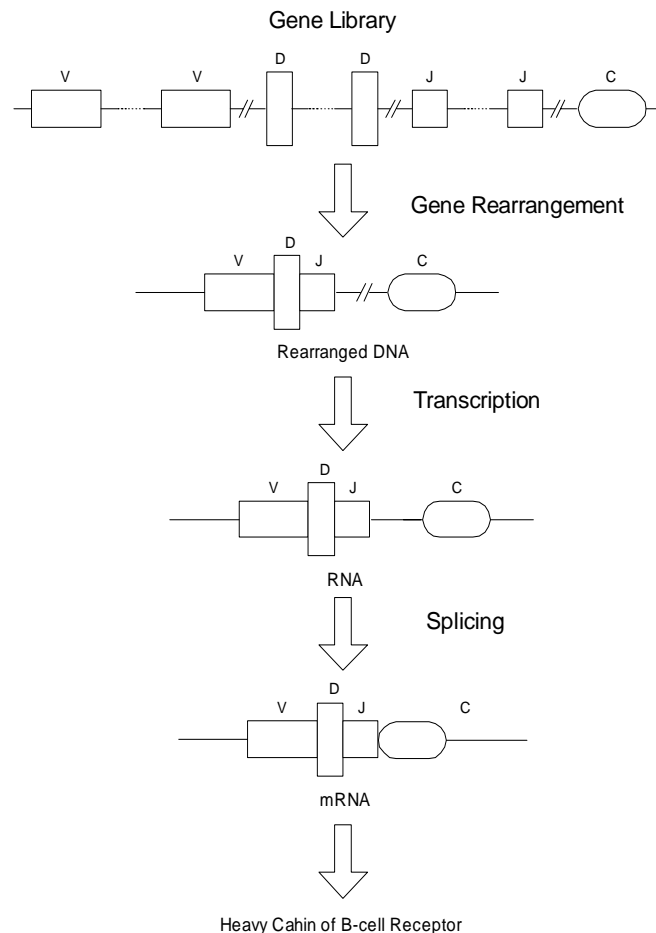


Figure A.3 B-Cell Receptor Genetic Organisation, [Opera, 1999]. The gene fragments randomly selected from gene library are rearranged. The rearranged gene fragments are joined by the transcription process. The splicing process joins the constant region, C, to VDJ and produces mRNA.

In order to create a unique receptor, single gene segments from individual gene libraries are randomly selected. The selected gene segments are joined and thus form a continuous gene sequence, called messenger RNA (mRNA) [Tizard, 1995]. This leads to exponential numbers of possible combinations of DNA gene segments expressed in mRNA. According to the mRNA produced, a unique receptor can be created. In addition to this basic mechanism, there are several other genetic mechanisms that increase the diversity, and B-cells and T-cells have slightly different mechanisms. After passing through all these various genetic mechanisms, embryonic lymphocytes develop into mature lymphocytes.

B-lymphocytes

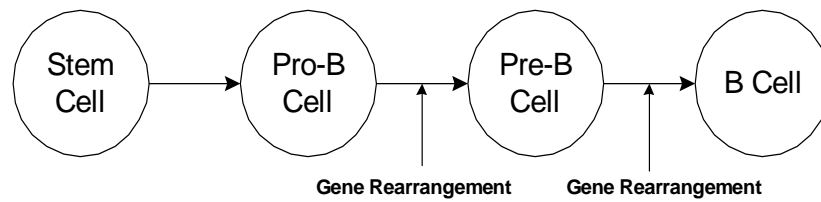


Figure A.4 B-cell development

B-cells develop in bone marrow. The B-cells are named after the 'B' of 'B'one marrow. Until a B-cell matures and develops into an antibody secreting cell, it passes through several different development stages. The first stage starts by the presence of a stem cell in bone marrow. The stem cell is innate and retains the embryonic ability to differentiate into a pro B-cell. The pro B-cell initially selects and rearranges the gene segments that encode the heavy chain of antibody. After the completion of this first gene rearrangement, the pro B-cell is differentiated into pre B-cell and the pre B-cell select and rearranges the gene segments which encode the light chain of antibody [Tizard, 1995; Paul, 1993; Roitt *et al.*, 1998].

Apart from these basic gene rearrangement mechanisms, B-cells adopt several strategies to increase their diversity [Roitt *et al.*, 1998; Tizard, 1995]. Firstly, B-cells choose one of two different light chains. There exist two distinct classes of light chains, κ and λ . The mRNA of the B-cell antibody receptor is formed by a heavy chain and either a κ light chain or a λ light chain, but not both. In the pre B-cell stage, a *progressive series of gene rearrangements* occur. This prevents the chance of creating a new light chain being missed. Not all the combinations of selected gene segments succeed to produce mRNA during the development of a light chain. The failure of transcribing to mRNA results in the failure of creating a new receptor. To prevent this, pre B-cells have several additional opportunities to produce antibody receptors. Pre B-cells initially attempt to rearrange the genes of a κ light chain. If they fail, they select different gene segments from the κ light chain. If both attempts fail, then pre B-cells switch their attention to the λ light chain. Similarly, pre B-cells attempt to rearrange selected genes from the λ light chain and if they fail, they select other gene segments from the λ light chain. When the four attempts have failed, the generation of a new antibody receptor fails. Pre B-cells increase the diversity of antibody receptors by allowing them to have several progressive chances of gene rearrangements.

As the second strategy, pro B-cells and pre B-cells choose different joining positions. The gene segments selected from V, J, and D regions and each region has special joining sites. When the gene segments of different regions are joined, the portions of gene segments from the joining

sites to the ends of gene segments are looped out. The looped out gene segments are chopped out, resulting in V region gene segments joined directly with J region gene segments, and J region gene segments directly joined with D region gene segments. Pro B-cells and pre B-cells select *different joining positions* of each gene segment when they generate mRNA and this certainly creates more diverse gene combinations. Furthermore, some new random genes can be inserted or deleted from the joining sites after chopping out the joined loop. We call this *base insertion*.

Another strategy is *somatic mutation*. V region genes can be mutated at random in many points. If this new antibody receptor generated via V region gene mutation fails to bind any antigen, then this antibody dies off. In contrast, if this antibody binds any antigen, it survives and proliferates. The details of proliferation are discussed in the later section A.1.5 Evolution. While the general mutation rate in gene natural selection is very low, the mutation rate of V region genes is high. One mutation occurs each time a B-cell is developed. This is why this mutation is called somatic mutation.

Apart from the diversity of variable regions, the diversity of constant regions is also maintained. Constant region genes are selected independently from V region genes. After finishing the selection of VDJ gene segments, C region gene segments are selected from C region gene libraries. The heavy chain has 5 different C region gene classes and the same VDJ gene segments can be joined with one of 5 different C gene classes. This leads to generating antibodies with the same specificity for antigens but different biological functions. This is called *class switching*. The significance of class switching is that the same antigens subjected to various different forms of attack are detected and handled in a different way. For example, two antibodies that have the same V domain genes can have two different constant region genes, which make one antibody circulate in the blood and body tissues and another antibody secreted be across mucous membranes to provide protection in the gut and lungs. Therefore, two antibodies can detect antigens having same specificity, but residing in different places.

T-lymphocytes

T-cells are also differentiated from stem cells and are developed in the thymus, hence the name T-cells. During the development processes in the thymus, T-cells transcribe DNA into mRNA. The diversity of T-cell receptors is maintained in a similar way to B-cell's [Tizard, 1995; Roitt *et al.*, 1998; Playfair, 1996]. T-cells select gene segments from DNA and rearrange, insert and delete them to produce mRNA. They also loop out the joining sites and chop them out when V-J-D regions are joined. Similarly, they choose various joining positions, insert or delete random genes and perform class switching. But, there is one major difference between the generation of

diversity of B-cell receptors and T-cell receptors. Somatic mutation does not occur in T-cell receptor development. When T-cells are developed, they also follow hierarchical development stages. T-cells first rearrange the gene segments from γ and δ chains. If this fails to produce a new receptor, then T-cells switch to α and β chains. Like B-cells, T-cells also attempt to make different chain combinations to prevent missing chances.

Another important feature of T-cell development is that an immature stem cell develops into two different T-cells [Paul, 1991]. If a stem cell in the thymus contains the CD4 protein, it is developed into a CD4 T-cell and if a stem cell in the thymus contains the CD8 protein, it is differentiated into a CD8 T-cell. These two different types of T-cells play different roles. CD4 T-cells act as helper T-cells and CD8 T-cells act as killer T-cells.

A.1.4 Activation

Both antigens on the surface of foreign cells and antigens inside self cells are recognised by B-cells and T-cells. This recognition triggers the immune response to kill recognised antigens. More precisely, the human immune system employs approximate binding to trigger actual immune response. The approximate binding allows immune systems to detect numerous different antigens by one B-cell antibody or T-cell [Forrest and Hofmeyr, 2001].

B-lymphocytes

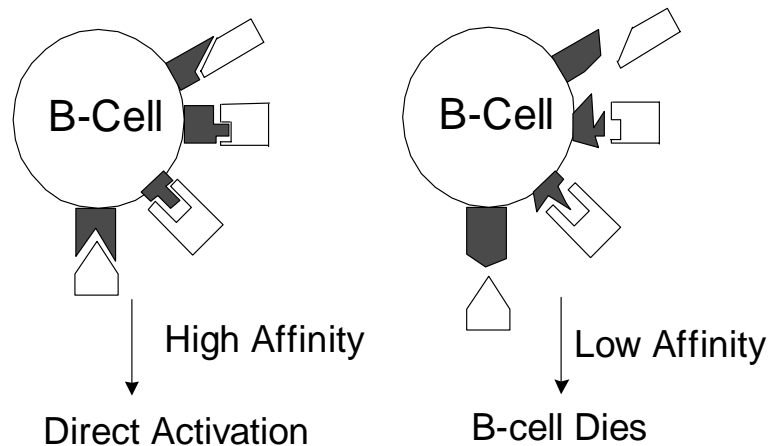


Figure A.5 B-Cell Activation

The antibodies of mature B-cells are activated by the epitopes of antigens. They can be directly activated or indirectly activated with the assistance of helper T-cells [Forrest and Hofmeyr, 2001; Paul, 1993]. The receptors on one lymphocyte have an identical structure and the number of receptors which bind to an antigen determines the affinity between a given lymphocyte and antigen. As many receptors match epitopes, the affinity is higher. Similarly, as fewer receptors match epitopes, the affinity is lower. There is a threshold of affinity that determines a direct activation or an indirect activation. When a B-cell binds to an antigen with strong affinity above

a threshold, it directly causes this B-cell to activate, grow and differentiate. On the other hand, if a B-cell binds to an antigen with weak affinity below a threshold, it needs the help of a helper T-cell to be activated. Therefore, different antigens, which are not the same but similar enough, can be detected by the approximate binding of a single antibody.

T-lymphocytes

As discussed before, while B-cells are activated by binding to antigen epitopes, T-cells are activated by binding to MHC molecules [Paul, 1993; Playfair, 1996]. MHC has two classes known as Class I and Class II, and they are slightly different in structure. The Class I MHC molecule is recognised by CD8 T-cells and the class II MHC molecule matches CD4 T-cells. When a CD8 T-cell binds Class I MHC on the surface of infected host cell, the CD8 T-cell kills this infected cell. On the other hand, a CD4 T-cell binds Class II MHC and it acts as a helper cell. When a B-cell binds to an antigen with weak affinity, a fragment of the antigen is delivered to a Class II MHC on the B-cell's surface. When this Class II MHC binds to a CD4 T-cell, the CD4 T-cell sends a chemical signal to a B-cell which allows the B-cell to activate, grow and differentiate. The T-cell's role as a helper cell is the main reason why T-cells do not mutate during their development. B-cells that are newly generated through somatic mutation are tested by helper T-cells, and thus helper T-cells never obtain new genes through mutation.

A.1.5 Evolution

B-cells and T-cells employ various gene shuffling mechanisms and somatic mutation in their development stage. This is the strategy for maintaining the diversity of antibodies. Besides these mechanisms, human immune systems adopt different strategies for the same purpose. As one species evolves via natural selection, human immune systems also evolve through a process called *clonal selection*. The genes, which determine the specificity of antibodies, continuously evolve toward having the capacity to detect more prevalent pathogens at any moment and reproduce new lymphocytes with high affinity for those specific pathogens [Playfair, 1996; Roitt, *et al.*, 1998, Tizard, 1995].

When B-cells are developed in bone marrow, only a limited energy source is given to them. They are active immediately after released from bone marrow, but they are rapidly exhausted and die. However, they do not simply disappear if they are activated by binding to specific antigens. When B-cells are directly or indirectly activated by antigens, they are divided and differentiated into a number of clones of antibody secreting cells, plasma cells, before they are exhausted. Plasma cells can have the same antigen-binding properties as the receptors of parent B-cells or they can have mutated antigen-binding properties. As B-cells bind more to antigens, they have more chances to be selected for cloning. Similarly, as they bind less to antigens, they

have fewer chances to be selected to clone and eventually tend to decrease. According to the different population of existing antigens, only the fittest antibodies survive.

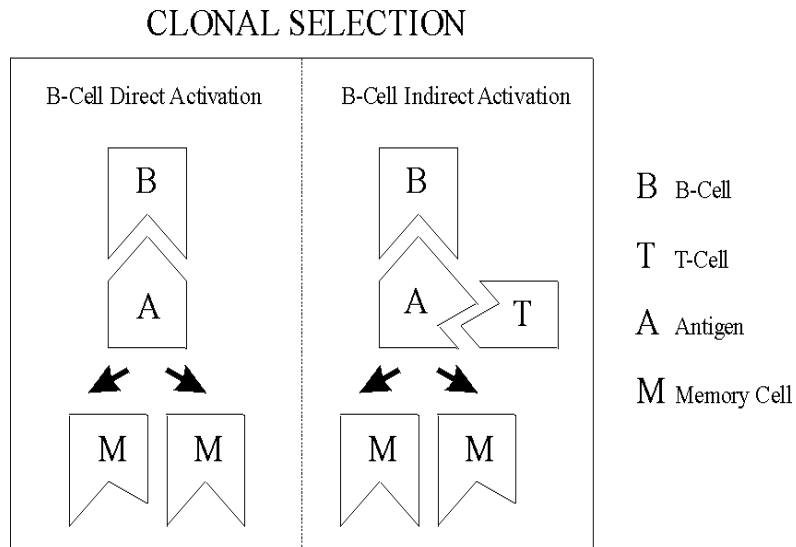


Figure A.6 B-cell Clonal Selection

Furthermore, when B-cells are activated by antigens, they produce memory cells for the reoccurrence of the same antigens. The life of B-cell and its clone, the plasma cell, is relatively short. However, some of the B-cell clones survive as memory cells. They have a special gene called *bcl-2* which is absent in short-lived B-cells and plasma cells. The *Bcl-2* gene enables the memory cell to survive for a longer time, such as several years. Some of the memory cells are exposed to antigens and differentiated into plasma cells without undergoing somatic mutation and other memory cells undergo somatic mutation to be differentiated into plasma cells. Particularly the plasma cells generated without somatic mutation allow the secondary response of immune systems. When new pathogens are detected by B-cells, they generally take some time. This is called the primary response. Compared to the primary response, the secondary responses by memory cells are very fast and efficient. Moreover, memory cells provide an associate memory property [Forrest and Hofmeyr, 2001]. The new antigens have a structure that is not the same but is similar to the structure of previously detected antigens, and can be detected by memory cells. This is because the binding of antibody and antigen is approximate. For example, when a body is infected by cowpox, the immune system takes time to detect and eliminate it. But if somebody is infected by smallpox after being infected by cowpox, he/she is rapidly cured by the secondary response of immune system. This is because cowpox and smallpox are similar enough to induce secondary response by memory cells.

A.1.6 Self Tolerance

One of the key features of the human immune system is self tolerance. New B-cell antibody receptors are randomly generated via somatic mutation. Therefore, there is the possibility for

randomly generated antibodies to bind to self cell antigens. This can lead to the killing of essential self cells and this causes autoimmune disease. However, autoimmune disease is relatively rare because human immune systems are equipped with self tolerance mechanisms [Life, 1993; Paul, 1991].

T-lymphocytes

As described above, when stem cells develop into T-cells in the thymus, they pass through several stages such as gene rearrangement. The embryonic T-cells also have to pass through the last test, negative selection, before leaving the thymus as mature T-cells. The thymus is an organ located just behind the breastbone and most of the self cells are circulated through the thymus. The maturing T-cells, through gene shuffling, base insertion and class switching, are tested to see if they bind the epitopes of self cell antigens. If maturing T-cells match self cells, these T-cells are eliminated. This process is called, *clonal deletion* or *negative selection*. The activation of clonal deletion also occurs according to the binding affinity between T-cells and self cells. The negative selection guarantees that maturing T-cells leaving the thymus are tolerant against self cells visited in the thymus before [Life, 1993; Paul, 1991; Tizard, 1995].

However, there is a flaw of clonal deletion. Even though most of the self cells are circulated through the thymus, there are still some cells which do not pass through the thymus. T-cells in the thymus cannot be tested against all existing self cells. Complete immune response by killer T-cells is triggered by not only T-cell receptors and MHC molecule binding but also some other protein binding. When T-cell receptors bind only to MHC molecules, they suppress antigen-presenting cells rather than killing them. However, when the CD28 protein on the surface of killer T-cells and the B7-20 protein on the surface of antigen-presenting cells bind together with binding between T-cell receptors and MHC molecules, the killer T-cells kill antigen-presenting cells [Life, 1993; Paul, 1991].

B-lymphocytes

B-cells also have a tolerance mechanism. Like the T-cell, B-cells perform their negative selection in the bone marrow. After gene rearrangement, when maturing B-cells match a self cell antigen, they are eliminated. This tolerance mechanism is applied to only maturing B-cells in the bone marrow. New B-cells can be generated from bone marrow or by cloning and mutation when they activate. In the latter case, B-cells do not pass negative selection but they can be self tolerant with the assistance of helper T-cells [Life, 1993; Paul, 1991].

Regulation of Immune Response

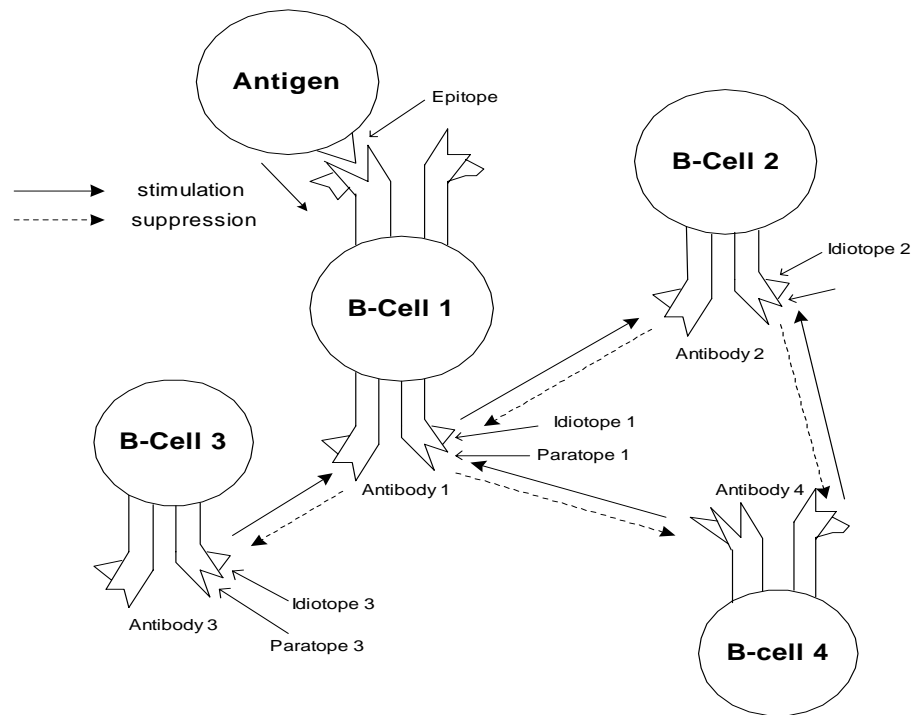


Figure A.7 Jerne's Immune Network, [Timmis, 2001]

In addition to the B-cell and T-cell tolerance mechanism, human immune systems provide a mechanism to regulate the magnitude of an immune response. An insufficient number of antibodies can cause immunodeficiency and increase susceptibility to infection. On the other hand, an excessive number of antibodies can lead them to kill essential self cells and cause autoimmune disease. Therefore, the development of antibodies should be regulated not only by quality but also by quantity [Paul, 1991]. Idiotypic antibodies can play the role of controlling the quantity of antibodies [Paul, 1993; Playfair, 1996]. Idiotypic antibodies bind to other antibodies rather than binding to antigens. The binding area of antibody receptors, the V-domain, has the particular shape that is commonly complementary to both antigen epitopes and other antibody receptors. Thus, antigens and other antibodies compete for the chance to bind to a specific antibody. When an antibody receptor binds to an antigen epitope, this is called a *paratope*. In contrast, when an antibody receptor binds to another antibody receptor, this is called an *idiotope*. The definition of two different types of antibody is only a matter of convenience. Immune systems let antigens and anti-antibodies compete to bind to antibodies and the winning anti-antibodies can suppress the binding between antigen and antibody, to trigger immune responses. The inhibition of idiotype antibodies against antigens, triggering immune responses, contributes to regulate an appropriate level of immune responses.

A.1.7 Distributed Detection

The overall 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 order to complete the overall immune process. For example, the acquired immune system handles pathogens via the interaction between B-cells, T-cells and other cells such as complements and macrophages. While B-cells and T-cells recognise antigens, macrophages and complements remove the detected antigens. This co-operation between millions of different cells implies that the human immune system is distributed [Playfair, 1996].

Lymphoid System

All the cells involved in natural and adaptive immune responses originate from stem cells in bone marrow. The original stem cells are divided into various types of immune cells including T-cells and B-cells. When B-cells are released from bone marrow, they are completely mature and circulate via the bloodstream. On the other hand, some stem cells are developed into pre T-cells in bone marrow and go to the thymus for complete maturation. Like B-cells, pre T-cells complete their maturation in the thymus, leave the thymus and circulate around the body through the bloodstream. Lymphocytes, including both B and T, continuously circulate around the body in the blood and encounter antigens leading to their activation and evolution in lymphoid organs. The bone marrow, blood and lymphoid organs are collectively known as the *lymphoid system*. In particular, we bone marrow and the thymus are called *primary lymphoid organs*, where the lymphocytes are developed. Lymphocytes generated in primary lymphoid organs migrate to *secondary lymphoid organs* such as lymph nodes, spleen, tonsils and lymphoid tissues in the intestine, the lungs, and other body surfaces. In secondary lymphoid organs, mature lymphocytes encounter foreign antigens and they are activated and show immune responses [Tizard, 1995; Playfair, 1996].

Interaction with Other Cells

Apart from B-lymphocytes and T-lymphocytes, many other cells co-operate to complete the overall immune mechanism [Playfair, 1996]. Even though lymphocytes are activated by antigens, very few antigens appear directly to lymphocytes. Instead, they are conveyed to lymphocytes by other cells such as dendritic cells and macrophages. They are collectively called *antigen-presenting cells*. They trap antigens circulating in the lymphoid system and in non-lymphoid tissues and convey antigens to lymphocytes in lymphoid nodes. Therefore, by the help of antigen-presenting cells, even antigens not found in lymph nodes can activate B-cells and T-cells. In addition to the antigen-presenting cells, some other cells also help B-cells and T-cells.

They mainly help B-cell and T-cells to eliminate antigens. Even though killer T-cells can kill antigens without the help of other cells, when B-cells are activated by antigens, they also react to other cells which have the capacity to kill antigens.

Immune Network

Jerne, an Immunologist, proposed immune network theory that theoretically synthesises the distributed detection feature of immune systems [Jerne, 1974]. He views immune systems as a functional network of lymphocytes and the network at any moment shows the dynamic state of internal interactions of lymphocytes, antibodies and antigens. In other words, when antibodies bind to antigens, they divide and proliferate. These antibody clones can bind to antigens again and divide and proliferate or bind to anti-antibodies and remain suppressed and decay. The continuous chain of differentiation by antigens and suppression by anti-antibodies can form a large-scaled network. And finally when this network reaches the equilibrium status between suppression and stimulation, it determines the overall immune system. This theory particularly emphasises the parallel and distributed feature of immune systems. It addresses the fact that the millions of local immune responses between a single antibody and a single antigen or a single anti-antibody occur in parallel and in scattered places and these interactions lead to the final appropriate level of immune responses.

A.1.8 Summary of Human Immune Systems

In this section, the sophisticated immune mechanisms of human immune systems are divided into several stages and described accordingly. The stages are such as recognition, genetic structure and development, activation, evolution, self tolerance and distributed detection. Even though the above description is simplified, it is still difficult to understand the entire system collectively, particularly with respect to the relations between individual stages. In this section, these complicated mechanisms are simplified to help understanding the entire human immune system.

The human immune system has a multi-layered architecture, consisting of natural immune systems and adaptive immune systems. The natural immune systems are innate and ever present, while adaptive immune systems are dynamically generated against the non-self organisms encountered. In particular, lymphocytes from adaptive immune systems play a central role in recognising harmful antigens. Lymphocytes can be classified into two main types according to function: B-lymphocytes and T-lymphocytes. B-lymphocytes are antibody secreting cells and T-lymphocytes can kill antigens or help or suppress the development of B-lymphocytes. B-lymphocytes have specific binding areas that have complementary shapes to the epitopes of antigens and a specific antigen is recognised by its epitopes binding to B-

lymphocyte antibody receptors. On the other hand, T-lymphocytes detect particular antigens hidden inside human host cells by binding its receptors to MHC molecules, which collect the fragments of hidden antigen proteins.

Both B-lymphocytes and T-lymphocytes have their own unique gene structures and gene libraries comprising these structures. Both B-cells and T-cells are made up several of chains and each chain has a variable domain and a constant domain. The genes in a variable domain are highly variable from one to another and this determines the specific binding area to antigens. The genes in the constant domain are invariable and show various biological effects when B-cell antibody receptors bind to antigen epitopes.

B-cells and T-cells are originated from stem cells. B-cells and T-cells are developed in bone marrow and the thymus respectively by selecting gene segments randomly and joining them. Furthermore, they adopt a progressive series of gene rearrangements, base insertion, choosing different joining sites and class switching during their development processes. T-cells are developed into two different types: killer T-cells and helper T-cells. One major difference between B-cell development and T-cell development is that only B-cells perform somatic mutation to increase their diversity. This is because T-cells act as helper T-cells, which determine whether B-cells divide into other clones or not when they bind to antigens with weak affinity. Maturing B-cells and T-cells have to pass the last test, negative selection, before leaving bone marrow and the thymus. If maturing B-cells and T-cells bind to self cell antigens, they are eliminated.

Mature B-cells and T-cells that pass the negative selection are released from bone marrow and the thymus respectively. Both B-cells and T-cells continuously circulate around the body in the blood and encounter antigens for activation and evolution in secondary lymphoid organs. The antibodies of B-cells, which recognise harmful antigens by binding to them, are activated directly or indirectly. When B-cell antibody receptors bind to antigen epitopes with strong affinity above a threshold, they are directly activated. On the other hand, B-cell antibody receptors can bind to antigen epitopes with weak affinity below a threshold, when a fragment of antigen is delivered to Class II MHC on the B-cell surface. When this MHC binds to a helper T-cell, the helper T-cell sends a chemical signal to a B-cell which allows the B-cell to activate, grow and differentiate. In addition, when killer T-cells bind to Class I MHC on the B-cell surface, they kill this infected B-cell.

With or without the assistance of T-cells, B-cells are activated and this activation is immediately followed by clonal selection. The activated B-cells are divided into a number of clones that have the same antigen-binding properties as parent B-cells or mutated antigen-binding properties. On

the other hand, if no antigen activates B-cells within a limited time, they rapidly die off. Therefore, according to the existing antigens, only the fittest B-cell antibodies survive. The initial generation of B-cell antibodies is generally a wasteful process. B-cells evolve via clonal selection. In contrast, idiotype antibodies can activate antibody receptors. Immune systems let antigens and anti-antibodies compete to bind to antibodies and the winning anti-antibodies can suppress binding between antigen and antibody. The inhibition of idiotype antibody against antigen contributes to regulate an appropriate level of immune responses. Jerne, an Immunologist, proposed an immune network theory based on understanding the role of the idiotype antibody. He views immune systems as a functional network of lymphocytes whose state at any moment consists of internal interactions between lymphocytes, antibodies and antigens. The continuous chain of differentiation by antigens and suppression by anti-antibodies can form a large-scaled network. Finally when this network reaches the equilibrium status between suppression and stimulation, it determines the overall immune system. Furthermore, when antigens activate B-cells, they produce memory cells for the reoccurrence of same antigens in the future. The secondary responses by these memory cells are highly efficient and have the property of associated memory.

Appendix. B.

Discussion of The Artificial Immune Model

To provide an indication of the advantages of the artificial immune model proposed in chapter 3, the new artificial immune model is now analysed with respect to the requirements of a network-based anomaly detector. Kim and Bentley [Kim and Bentley, 1999a] described the seven requirements of a competent network-based IDS. The proposed artificial immune model is assessed with respect to these seven requirements. The argument provided here is based on a comprehensive study of literature.

The proposed artificial immune model is distributed by using a unique detector set in a local secondary IDS for detecting local intrusions and employing communications among secondary IDS's for detection of network intrusions. This distributed feature allows the model to be robust, configurable, extendible and scalable. Firstly, the artificial immune model is *robust*. The failure of any detector set residing at any local host does not cripple an overall artificial immune system even though it may cause some minor degradation of detection accuracy. Each detector set can still detect network intrusions even after the failure of the primary IDS. This is because each local host already has detector sets, which were transferred before the failure. Besides, if an intruder breaks through a local host and gains the information about how detectors describe anomalous behaviour, this intruder might attempt to use this information to disguise his or her activities. However, the uniqueness of each detector set makes this kind of attempt difficult. Secondly, it is *configurable*. Even though detectors are generated in the primary IDS, their usefulness is proved at a local level by employing clonal selection in each secondary IDS. Furthermore, this local level clonal selection drives the gene library evolution in the primary IDS. In other words, the generated detectors co-evolve to detect various intrusions and this co-evolution is led by the self profiles and existing intrusions in each local level. Therefore, the artificial immune model configures local requirements in a self-organised way disregarding various requirements of other hosts. Thirdly, it is *extendible*. When a new local host is added to a network, it simply needs to generate another detector set for the new host and install a secondary IDS consisting of an automated profiler, anomaly detection process, clonal selection process and a communicator without considering other hosts. These components are totally independent from the components at other secondary IDS's and thus they ensure that the artificial immune model is easy to extend. Fourthly, it is *scalable*. At initial stages, an artificial immune system might need to generate a large detector set. However, as it detects more and more anomalies, each local host will be equipped with more and more memory detectors and eventually will require very few new detectors to be transferred. Nevertheless, in practice this requires the occurrence of a number of various intrusions within a short time. Therefore, the overall artificial immune mechanisms may be simulated by presenting a number of intrusions

for a short time and this is used for the initial learning process before the launch of real intrusion monitoring by the artificial immune model.

In addition, the artificial immune model is self-organising by performing gene library evolution, negative selection and clonal selection. This property of self-organisation makes the model both *adaptable* and capable of *global analysis*. Firstly, the negative selection process allows detectors to dynamically consider the self information at any moment. The clonal selection and the gene library evolution generate various detector sets that are the fittest for the recently encountered intrusions. Therefore, the newly generated detectors always dynamically learn knowledge about currently existing intrusions and self. Furthermore, when a new intrusion is detected, these new abnormal patterns will be registered to the gene library of the primary IDS and remain as the memory detectors at the secondary IDS's. Therefore, the artificial immune model still can be highly adaptive. Secondly, global analysis is achieved via the communication between the primary IDS and the secondary IDS's and this communication mechanism is simple and autonomous, which does not require a global communication controller. Finally, the artificial immune model is *lightweight* by detecting various intrusions using approximate binding and memory cells, performing gene library evolution and gene expression¹. This lightweight feature provides good *efficiency*. Firstly, the approximate binding permits one detector to detect a number of different intrusions. Consequently, the model needs to generate a much smaller number of detectors than the number of intrusions that are expected to be detected. Secondly, as mentioned above, clonal selection generates memory detectors within local hosts. As the number of memory detectors increases, the number of new detectors required will decrease, resulting in a reduction of computation time. More importantly, as the detection of intrusions continues, a gene library collects useful genes. Through gene library evolution, these genes define detectors that have already proved their usefulness by identifying anomalies. Since such detectors use only the most useful features of the profile at any one time, this removes the need for each local host to perform feature selection during profiling. This feature certainly reduces the overheads of local monitored hosts compared to the co-operative approach. The final example of efficiency in the system is provided by the gene expression process. This process allows the artificial immune model to generate a huge number of detectors from a small number of genes in the gene library.

¹ Even though the novel evolutionary approach of the artificial immune model allows the secondary IDS's to be lightweight, it may impose some more work on the primary IDS. To resolve this problem, it may be designed as a parallel array of the primary IDS's. For example, the first router which receives all network input packets outside a network domain can split network packets into groups of flow based on each connection. Then a number of different flow groups can be sent to each primary IDS. Each primary IDS will have the identical components that have been introduced in this paper and it generates specific detector sets and self profiles based on each connection. The specific detector sets and self profiles generated by an individual primary IDS are sent to the second router and this router can transfer them to a specific secondary IDS (a local host) within a domain.

Appendix. C.

The Fields of Network Traffic Self-Profiles

The following are the 33 fields that defined self profiles used in Chapter 4 Negative Selection Algorithm.

| Field | Type | Description |
|------------------------|----------------------|---|
| Connection ID | Numerical | ID identifies each connection. |
| Src_addr | Nominal | Source address |
| Src_port | Nominal | Source port number |
| Dest_addr | Nominal | Destination address |
| Dest_port | Nominal | Destination port number |
| Server | Boolean | True when a source host is a server. |
| Src_user_app | Boolean | True when a source port is a user application. |
| Src_port_vulner | Nominal | 5 different types of source port vulnerabilities. |
| Src_port_firewall | Nominal | 6 different types of source port firewall strategies |
| Dest_user_app | Nominal | True when a destination port is a user application. |
| Dest_port_vulner | Nominal | 5 different types of destination port vulnerabilities |
| Dest_port_firewal l | Nominal | 6 different types of destination port firewall strategies |
| NumberOfPackets | Interval | The number of sent packets for one direction of one connection |
| Duration | Interval | Duration of one direction of one connection |
| PacketRate | Interval/ Ordinal | The rate of number of sent packets per one direction of one connection (= NumberOfPackets / Duration) |
| SentSYN | Interval | The number of SYN for one direction of one connection |
| SentFIN | Interval | The number of FIN for one direction of one connection |
| SentRST | Interval | The number of RST for one direction of one connection |
| SentPUSH | Interval | The number of PUSH for one direction of one connection |
| SentPUSHrate | Interval/ Ordinal | The rate of number of PUSH / number of packets for one direction of one connection |
| Duplicate | Interval | The number of duplicate packets for one direction of one connection |
| RateDuplicate | Interval/ Ordinal | The rate of duplicate packets for one direction of one connection (= Duplicate / NumberOfPackets) |
| Missing | Interval | The number of missing packets for one direction of one connection. |
| RateMissing | Interval/ Ordinal | The rate of missing packets for one direction of one connection (= Missing/ NumberOfPackets) |
| OutOfOrder | Interval | The number of OutOfOrder for one direction of one connection |
| RateOutOfOrder | Interval/ Ordinal | The rate of OutOfOrder for one direction of one connection |
| Bytes | Interval | Bytes of sent packets for one direction of one connection |
| BytesRate | Interval/ Ordinal | The rate of sent bytes per one direction of one connection (= bytes / duration) |
| ConnectionReject ed | Interval | The number of SYN when an initiator host did not receive acknowledgements for one connection |
| SYNerror | Interval | For one connection, the number of sent SYN as acknowledgements when an initial host did not request the initiation of connections. |
| Termination | Nominal | Termination type: normal, finFailure, finMistake, resetTerm, pushTerm, resetError, finaAckMissing, cutting |
| WrongSize | Interval | The number of directions whose received bytes are larger than available buffer sizes within a connection |
| RateWrongSize | Interval | The rate of directions whose received bytes are larger than available buffer sizes within a connection (= wrongSize / duration) |

Appendix. D. Setting Activation Threshold and Life Span Values in DynamiCS

The section 6.5 Experimental Results 1: Examination of Complete Antigen Data presents thorough study of three important parameters of DyanmiCS: toleration period (T), activation threshold (A) and life span (L). Consequently, the experimental results suggest that if in a particular application the first priority is a low false positive error rate, and secondly the true positive detection rate, a T value that is large enough to show a sufficient FP rate should be found first regardless of A and L values. This section provides additional discussion of how A and L can be chosen. The following discussion considers the situation when T is set to a fairly large value in order to obtain a satisfactory FP rate.

After a satisfactory FP rate is obtained by tuning T , A and L can be changed in order to get a satisfactory TP rate while still maintaining the FP rate. For instance, if there is a case showing a low FP rate but also presenting an unacceptably low TP rate, both lowering A and increasing L can guide the system to attain a higher TP rate. Lowering A or increasing L affects the total number of detector activations. However, these two similar outcomes have slightly different features. In the first case, lowering A without increasing L , mature detectors activate when they match a smaller number of antigens that exist for a relatively short period. Thus, memory detectors produced in this case will remember more specific antigen niches existing only for a relatively short period. In contrast for the latter case, increasing L without decreasing A , mature detectors activate when they detect a sufficient number of antigens occurring for a longer period. Accordingly, generated memory detectors will have information matching antigens existing in various antigen clusters. In summary, lowering A without increasing L leads the system to concentrate on matching more specific antigens, that is small niches of an antigen cluster selected for a short period of time. On the other hand, increasing L without lowering A lets the system detect large antigen niches possibly appearing for a longer period of time.

Consequently, the danger of only lowering A is that generated memory detectors will have information matching more specific and smaller antigen niches existing only for a short period. Thus, if any environment constantly and frequently alternates the antigen distribution, this type of memory detectors will not contribute to increase the TP rate in the future. This is because the antigens detected by these memory detectors possibly exist only for an initial short period and it cannot be guaranteed that they occur again in the future. However, this is not a serious problem as long as they do not detect self antigens in the future and it does not require too much resource to store memory detectors. Thus, a more important concern is whether it activates by mistakenly detecting self antigens in the future. However, this problem can be mitigated by giving a large T value (see figure 6.8). Therefore, lowering A when T is large enough is not such a dangerous

idea but can be wasteful. This is because it produces many memory detectors matching small niches in the non-self antigen set, and these are not guaranteed to appear again in the near future. This strategy might let the system keep many memory detectors that do not contribute noticeably to increase the TP rate. A more efficient strategy will keep memory detectors only when they are needed rather keeping them indefinitely. Therefore, this situation requires a way to handle generated memory detectors that aim to ensure that they exist only when they are needed. Another danger of only increasing L without lowering A is that all detector activations might omit to match small niches existing in an each antigen cluster (see figure 6.12).

The appropriate decisions about lowering A or increasing L , or both, will be different according to the given environment. For instance, if we know that the distribution of an antigen subset presented at each generation will appear again in a near future, lowering A can be a good idea that can boost TP rates by detecting small niches. However, if any situation shows that the distribution of antigen subsets presented over time changes substantially, lowering A and keeping memory detectors cannot be such a good idea. In addition, increasing T and L can also be equally bad for similar reasons. Since larger T and L imply keeping a larger number of immature and mature detectors that are not qualified to activate yet, increasing T and L can be an impractical idea, although they can reduce FP rate and generate more general and efficient detectors.

Appendix. E. Publications

The following eight papers were written as part of the research undertaken for this thesis.

1. Kim, J. and Bentley, P., (1999), "The Human Immune System and Network Intrusion Detection", *the Proceeding of 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT '99)*, Aachen, Germany, September 13- 19.
2. Kim, J. and Bentley, P., (1999), "The Artificial Immune Model for Network Intrusion Detection", *the Proceeding of 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99)*, Aachen, Germany, September 13- 19.
3. Kim, J. and Bentley, P. J., (1999), "Negative Selection and Niching by an Artificial Immune System for Network Intrusion Detection", *the Proceeding of A late-breaking paper, pp.149-158, Genetic and Evolutionary Computation Conference (GECCO '99)*, Orlando, Florida, July 13-17, 1999.
4. Kim, J. and Bentley, P. J., (2001), "Evaluating Negative Selection in an Artificial Immune System for Network Intrusion Detection", *the Proceeding of Genetic and Evolutionary Computation Conference 2001 (GECCO-2001)*, San Francisco, pp.1330 - 1337, July 7-11, 2001.
5. Kim, J. and Bentley, P. J., (2001), "Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator", *the Proceeding of the Congress on Evolutionary Computation (CEC-2001)*, Seoul, Korea, pp.1244-1252, May 27-30, 2001.
6. Kim, J. and Bentley, P. J., (2002), "Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Dynamic Clonal Selection", *the Proceeding of the Congress on Evolutionary Computation (CEC-2002)*, Honolulu, pp.1015 - 1020, May 12-17, 2002.
7. Kim, J. and Bentley, P. J., (2002), "Immune Memory in the Dynamic Clonal Selection Algorithm", to appear in *the Proceeding of the first International Conference on Artificial Immune Systems (ICARIS)*, September 9-11, 2002.
8. Kim, J. and Bentley, P. J., (2002), "A Model of Gene Library Evolution in the Dynamic Clonal Selection Algorithm", to appear in *the Proceeding of the first International Conference on Artificial Immune Systems (ICARIS)*, September 9-11, 2002.