Application of Immune Complement Algorithm to NSL-KDD Intrusion Detection Dataset

Najlaa B. Aldabagh **Mafaz M. Khalil**
College of Computer Sciences and Mathematics
University of Mosul

Received on: 22/06/2011 **Accepted on: 02/11/2011**

الملخص

تَتضمّنُ العديد مِنْ مشاكلِ العالم الحقيقي مسألة تحقيقَ الأمثلية الآنية للأهدافِ المُختَلفةِ والمتعارضةِ في أغلب الأحيان. وتَبْدو الخوارزمياتُ التطوّريةُ من الطرق الأكثر جاذبيةً لهذا الصنفِ مِنْ المشاكلِ، لأنها تقنيات تعتمد على الجيل الذي يمْكِنُه أَنْ يجدَ حلول وسطية متعدّدة في عملية تنفيذ واحدة، وهي لا تتطلّب أية فرضيات على دوال الهدف. من بين التقنياتِ الأخرى، أقترح في العقدِ الأخيرِ مثال جديد مستند على محاكاةِ سلوكِ نظامَ المناعة. وظهرت فيه أعمال رائدةِ، في العديد مِنْ التطبيقاتِ المختلفة.

يقدم هذا البحث وصفاً لنظام كشف تطفل على غرار أساس المفاهيمِ الحيوية المستلهمة من النظام المناعي وهي الانتقاء السلبي، الانتقاء الايجابي، والنظام التكميلي. حيث بإمكان ميكانيكية الانتقاء الايجابي كشف أنماط الهجوم(الغير ذاتية)، بينما يكون عمل الانتقاء السلبي حذف الخلايا اللمفية الاصطناعية التي تتفاعل مع الأنماط الطبيعية (الذات). بينما يعتبر النظام التكميلي آلية فاعلة، فهي سلسلة من البروتينات تنتشر في الدمِّ ويَغطّي أنسجةَ السوائلَ المحيطةَ. أساس الفكرةَ هو باختيار فقط تلك الخلايا التي تتَعرف على المُستَضدّات للمُرور بعمليتين: عملية التقطيع وعملية الربط، تقوم عملية التقطيع بقطع الخلية التكميلية إلى اثنين من الخلايا الثانويةِ، بينما تربْط عملية الربط خليتين سوية لتشكيل خلية كبيرة. ليكون الهدف هو الحُصُول على كاشفاتِ التكملةِ يُمْكِنُها أَنْ تتَعرفَ فقط على أنماط الهجومَ من مجموعة بيانات NSL-KDD.

ABSTRACT

Many real world problems involve the simultaneous optimization of various and often conflicting objectives. Evolutionary algorithms seem to be the most attractive approaches for this class of problems, because they are usually population based techniques that can find multiple compromise solution in a single run, and they do not require any hypotheses on the objective functions. Among other techniques, in the last decade a new paradigm based on the emulation of the immune system behavior has been proposed. Since the pioneer works, many different implementations have been proposed in literatures.

This Paper presents a description of an intrusion detection approach modeled on the basis of three bio-inspired concepts namely, Negative selection, Positive selection and complement system. The Positive selection mechanism of the immune system can detect the attack patterns (nonself), while the Negative selection mechanism of the immune system can delete the Artificial lymphocyte (ALC) which interact with normal patterns (Self). The complement system is a kind of the effecter mechanism, which refers to a series of proteins circulating in the blood and bathing the fluids surrounding tissues. It establishes the idea that only those cells that recognize the antigens are selected to undergo two operators: cleave operator and bind operator are presented, cleave operator cleaves a complement cell into two sub-cells, while bind operator binds

two cells together and forms a big cell. To obtain Complement detectors can recognize only the attack patterns from the NSL-KDD dataset.

Key words: *Artificial immune system (AIS), Immune complement algorithm (ICA), Negative Selection (NS), Positive Selection (PS), Complement Detectors (DCs), NSL-KDD data set.*

1. Introduction

Our immune system has its main task the detection of the infectious foreign elements (called pathogens) that attack us, and defend us from them (in other words, its main task is to keep our organism healthy). Examples of such pathogens are bacteria and viruses. Any molecule that can be recognized by our immune system is called antigen. Such antigens provoke a specific response from our immune system. Lymphocytes are a special type of cells that play a major role in our immune system [4].

Computer Security is a field that has gained significance over the past few years, especially with the widespread internetworking of computers. One of the important aspects of computer security is the detection of intrusions and attacks. Hence, considerable amount of research works have been dedicated to the exploration of various possible methods for detection of intrusions and attacks. Of late, the intrusion detection systems, modeled on the basis of the Artificial Immune System, have gained prominence because of their promise to provide for feasible and efficient detection mechanisms [9]. The Artificial Immune System is modeled on the basis of the Natural Immune System found in living organisms.

Literature survey indicates that, for intrusion detection, most researchers employed a common algorithms to detect multiple attack categories with dismal performance in some cases. The set of Immune algorithms applied in the literature constitutes a very small subset of problem. Additionally, reported results suggest that much detection performance improvement is possible.

2. NSL-KDD Intrusion Detection Dataset

An intrusion detection system (IDS) is an important component of the computer and information security framework. Its main goal is to differentiate between normal activities of the system and behaviors that can be classified as suspicious or intrusive. The role of Intrusion Detection Systems (IDSs), as special-purpose devices to detect anomalies and attacks in the network, is becoming more important. The research in the intrusion detection field has been mostly focused on anomaly-based and misuse-based detection techniques for a long time. While misuse-based detection is generally favored in commercial products due to its predictability and high accuracy, in academic research anomaly detection is typically conceived as a more powerful method due to its theoretical potential for addressing novel attacks. In a misuse detection based IDS, intrusions are detected by looking for activities that correspond to known signatures of intrusive or vulnerabilities. On the other hand, the anomaly detection based IDSs detect attacks by observing deviation from the normal behavior of the system. Its work by comparing network traffic, system call sequence, or other features of known attack patterns [1].

In this paper, a comprehensive set of pattern recognition and immune learning algorithms will be evaluated on the NSL-KDD data set, which is a new data set that consists of selected records of the complete KDD data set and does not suffer from any of mentioned shortcomings. The KDDCUP'99 data set was created by processing the TCP dump portions of the 1998 DARPR Intrusion Detection

System(IDS) evaluation dataset, created by Lincoln Labs, U.S.A. They acquired nine weeks of raw TCP dump data. This was processed into about five million connection records to detect intrusions at the network level.

The KDD training dataset consists of approximately 4,900,000 single connection vectors each of which contains 41 features and is labeled as either normal or an attack, it contains a total of 24 attack types(connections) that fall into 4 major categories: Denial of Service Attack (DoS), User to Root Attack (U2R), Remote to Local Attack (R2L) and Probing Attack.

Some intrusion experts believe that most novel attacks are variants of known attacks and the signature of known attacks can be sufficient to catch novel variants. The training datasets contain a total number of 24 training attack types, with an additional 14 types in the test data only [9].

The study presented here will create detection models using a comprehensive set of pattern recognition and immune learning algorithms and select best performing (in terms of probability of detection and false alarm rates) algorithms for each attack category. It is a detection system will be attempted to improve the overall detection performance on the four attack categories as they exist in the NSL-KDD data sets. The new version of KDD data set, NSL-KDD (training and testing records) is publicly available for researchers through website [3].

3. Artificial Immune Systems

We can find quite different definitions of an artificial immune system (AIS) in the literature; one possible definition could be "Artificial immune systems(AIS) are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving" [8]. The artificial immune system paradigm is rather recent comparing to other artificial intelligence paradigms like Neural Networks, Fuzzy Logic or the genetic algorithms. AIS began in 1986 with Farmer, Packard and Perelson's paper on immune networks , but there was only in the mid-90's that it kept the attention of scientists [4].

What do we need if we want to implement an AIS framework? If we abstract the immune system in a simplistic way we have a population of different types of immune cells and interactions between them through receptors. For our AIS we therefore need to have a population, defined as a set, a way to describe each element of the set, its length, and a way to measure an interaction. To describe the population, we will use the concept of shape space (S); it is used in immunology to quantitatively describe the interactions between immune cells and antigens. An element of S is described by a set of Np parameters (length, width, charge, ...). To cover the whole shape-space, we actually need to generate N = kL different elements, where K is the size of the alphabet, L the length of one element of the set, and N is called the potential repertoire. As we have seen, one antibody can detect pathogens with similar structure, i.e. it is not bound to only one specific pathogen (imagine the number of antibodies we would need if each could detect only one given pathogen) [4].

There are a growing number of computer models called AIS to simulate various components of the immune system and the overall behavior from the biological point of view. The models based on immune system principles, such as the clonal selection theory, the immune network model or the negative selection algorithm, have been finding increasing applications in fields of science and engineering such as: computer security, virus detection, process monitoring, fault diagnosis, pattern recognition, etc[3].

The Immune system (IS) is thought to be able to classify cells that are present in the body as self and non-self cells. The IS is made of two distinct sets of components: the innate IS, and the adaptive IS. The innate immune system is so called because the body is born with the ability to recognize certain microbes and immediately destroy them. Our innate immune system can destroy many pathogens on first encounter. An important component of the innate immune response is a class of blood proteins known as complement, which has the ability to assist, or complement, the activity of antibodies. The innate immunity is based on a set of receptors encoded in the germinal centers and known as pattern recognition receptors (PRRs), to recognize molecular patterns associated with microbial pathogens, called pathogen associated molecular patterns (PAMPs). The PAMPs are only produced by microbes and never by the host organism, hence their recognition by the PRRs may result in signals indicating the presence of pathogenic agents. This way, the structures related to the immune recognition must be absolutely distinct from our own cells and molecules in order to avoid damage to tissues of the host. The consequence of this mechanism is that the innate immunity is also capable of distinguishing between self and non-self, participating in the self/nonself discrimination issue, and playing a leading role in the boost of adaptive immunity [5].

The adaptive IS is more complex. It produces a large number of randomly created detectors. A negative selection. mechanism eliminates detectors that match all cells present in a protected environment (bone marrow and the thymus) where only self cells are assumed to be present. Non-eliminated detectors become naive detectors; they die after some time, unless they match something (assumed to be a pathogen), in which case they become memory cells. Further, detectors that do match a pathogen are quickly multiplied (clonal selection); this is used to accelerate the response to further attacks [5].

The immune system is composed of a great variety of cells that are originated in the bone marrow, where plenty of them mature. From the bone marrow, they migrate to patrolling tissues, circulating in the blood and lymphatic vessels. Some of them are responsible for the general defense, whereas others are “trained” to combat highly specific pathogens. For an efficient functioning, it is necessary a continuous cooperation among the agents (cells). Figure 1 presents a structural division among the cells and secretions produced by the immune system.

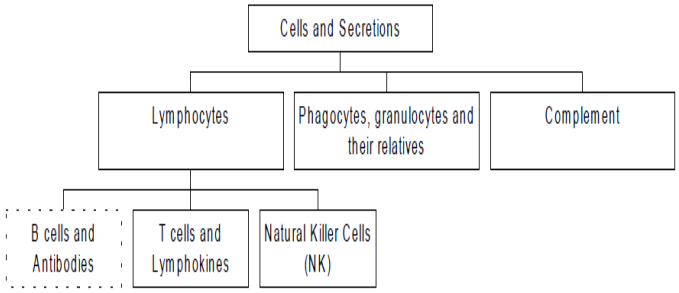


Figure 1: Structural Division of the Cells and Secretions of the Immune System.

The complement system, which represents a chief component of innate immunity, not only participates in inflammation but also acts to enhance the adaptive immune response. Specific activation of complement via innate recognition proteins or secreted antibody releases cleavage products that interact with a wide range of cell surface receptors found on myeloid, lymphoid and stromal cells. This intricate

interaction among complement activation products and cell surface receptors provides a basis for the regulation of both B and T cell responses . The activation pathways of the complement system are really evolution processes of complement proteins, in which, complement proteins cleave and bind, finally form a complex resulting in an impairment of osmotic regulation and subsequent cytolysis .In this paper, we follow a novel immunological algorithm based on the complement system-An Immune Complement Algorithm (ICA) as in [3], with some changes to serve our application. ICA mainly simulates the classical pathway of the complement system. In this algorithm, two operators: cleave operator and bind operator are presented, cleave operator cleaves a complement individual into two sub-individuals, while bind operator binds two individuals together and forms a big individual.

4. Immunologic Self/Non-self Discrimination

The immune system to function properly, it needs to be able to distinguish between the molecules of our own cells (*self*) and foreign molecules (*non-self*), which are *a priori* indistinguishable [2], Figure 2. If the immune system is not capable of performing this distinction, then an immune response will be triggered against the self-antigens, causing *autoimmune diseases*. Not responding against a self-antigen is a phenomenon called *self-tolerance*, or simply *tolerance* [5].

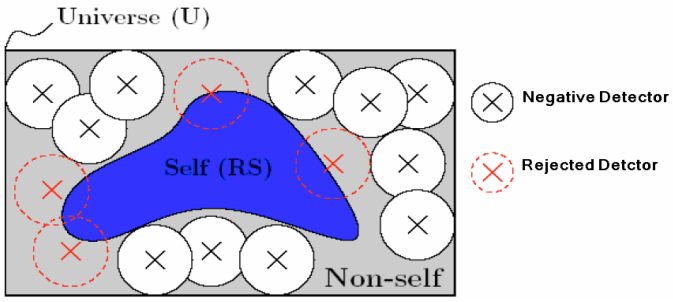


Figure 2: IS Self/Non-self Discrimination

4.1 Negative Selection Algorithms

One of the purposes of the immune system is to recognize all cells (or molecules) within the body and categorize those cells as self or non-self. The non-self cells are further categorized in order to induce an appropriate type of defensive mechanism. The immune system learns through evolution to distinguish between foreign antigens (e.g., bacteria, viruses, etc.) and the body's own cells or molecules. The purpose of negative selection (NS) is to provide tolerance for self cells. It deals with the immune system's ability to detect unknown antigens while not reacting to the self cells [5], (see Figure 3).

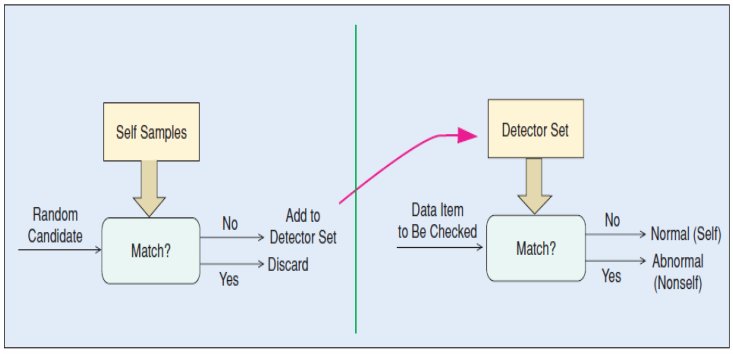


Figure 3: The Basic Concept of the Negative Selection (NS) Algorithm.

4.2 Positive Selection Algorithms

In contrast to NS, "positive detection techniques" are widely used in pattern recognition, clustering, and other domains, where they generate a set of detectors that match self-points (instead of non-self points). In this case, a model of the self-set (training data) is used to classify a sample as part of either self or non-self. A simple model of a positive detection (PS) could be built by using a nearest neighbor approach. If a point lies in a neighborhood of a sample self-point, then it will be labeled as belonging to the self-set [1], (see Figure 4).

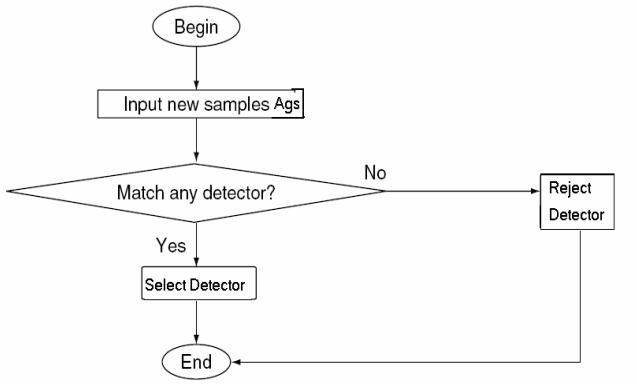


Figure 4: The Basic Concept of the Positive Selection (PS) Algorithm.

5. The Complement System

The complement system constitutes a complex formed by a set of circulating plasma proteins that complement the function of the antibodies. When the complement detects an invader organism, each of its components promotes a chain reaction (complement cascade). The result is a complex of proteins that bind to the surface of the invader causing lesions on its protecting membrane or facilitating the operation of phagocytes. It is formed by approximately 25 proteins that circulate inactively all over the body. Figure 5 illustrates the complement chain reaction [5].

The general properties of complement [8]:

- Present in all normal sera.
- Does not increase on immunization.
- Non-specific serologic reagent.
- Destroyed at 56°C in 30 mts.
- Not a single substance –complex.
- In classical pathway; complex is of 9 proteins.
- In alternate pathway; complex is of 13 proteins.
- Activation by antigen-antibody complex.
- Alternate pathway activated by polysaccharide/enzymes. Produces cytolytic destruction by specific antibody.
- Inactivators and inhibitors present in serum.

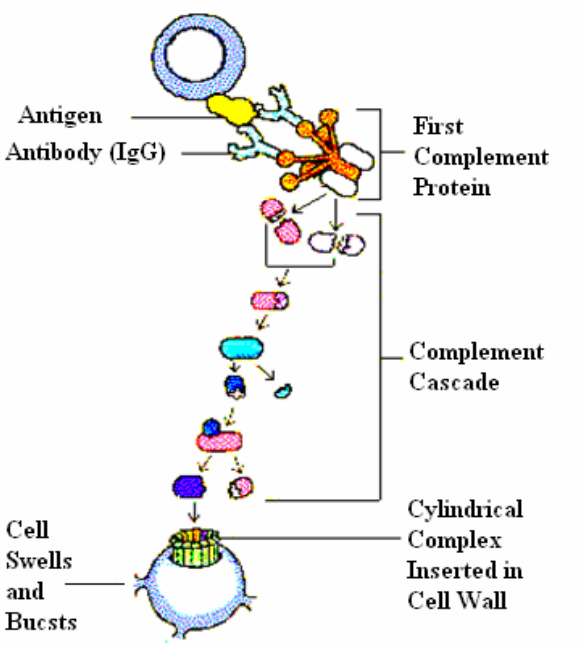


Figure 5: Complement Activation (cascade reaction)

The main functions or the biological effects of the complement system are[8]:

1) Chemotaxis: attraction of phagocytes to the sites of infection;
2) Opsonisation: the coating of an organism with proteins so as to make it palatable to phagocytes, by means of binding to specific complement receptors;
3) Anaphylaxis: increase in the blood flow to the infection sites and increase of vessel permeability;
4) Lysis. Damage in the plasma membrane of the cells(bacteria, and viruses). This macromolecular assembly is known as the Membrane Attack Complex (MAC).

All the above biological effects are realized through the complement pathways. There exists three complement activation pathways: the classical pathway, the lectin pathway, and the alternative pathway:

(i) The classical complement pathway is activated by antigen-antibody complexes.
(ii) The lectin pathway is activated by the interaction of microbial carbohydrates with mannose-binding proteins in the plasma and tissue fluids.
(iii) The alternative complement pathway is activated by C3b binding to microbial surfaces and to antibody molecules.

The pathways differ in the manner in which they are activated and ultimately produce a key enzyme called C3 convertase[3].

5.1 The Classical Pathway

The classical pathway of the complement system which is showed in the Figure 6, is activated by antigen-antibody complexes that have formed on the surface of a target cell. The classical pathway is composed of three phases: Identify phase, Activate phase and Membrane attack phase.

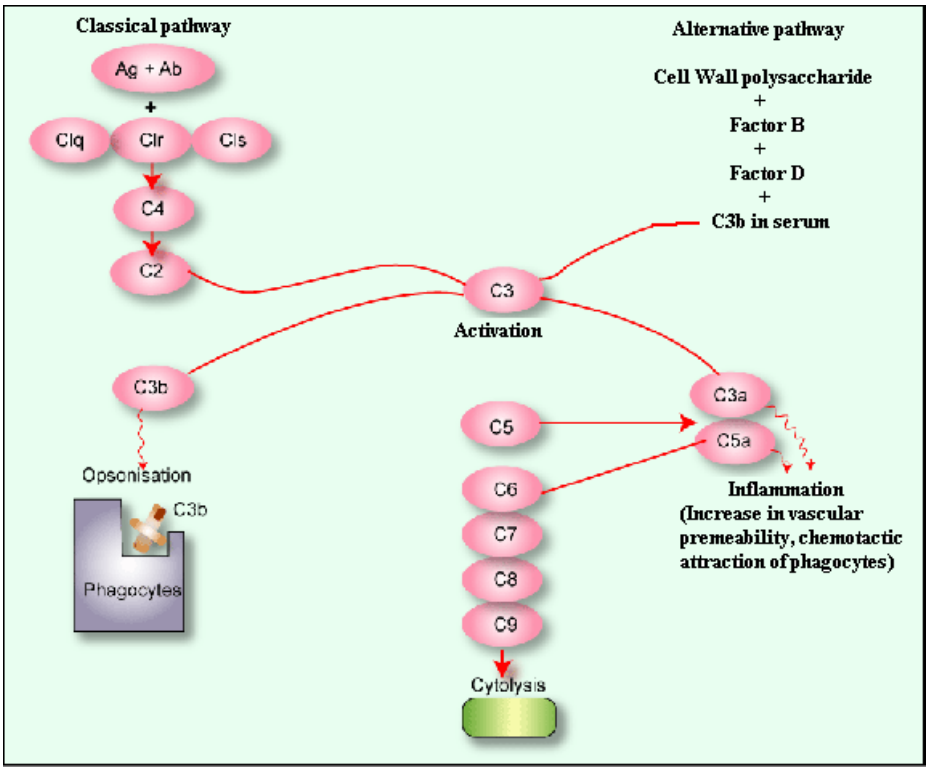


Figure 6: The Classical Pathway of the Complement System.

6. Pattern Recognition

From the point of view of pattern recognition in the immune system, the most important feature of artificial lymphocyte cells is that they have receptor molecules on their surfaces that can recognize antigens (either free or bound to an MHC molecule). In the B cells case, the receptor is an immunoglobulin, or antibody, molecule embedded in the membrane of the cell [5], see Figure 7.

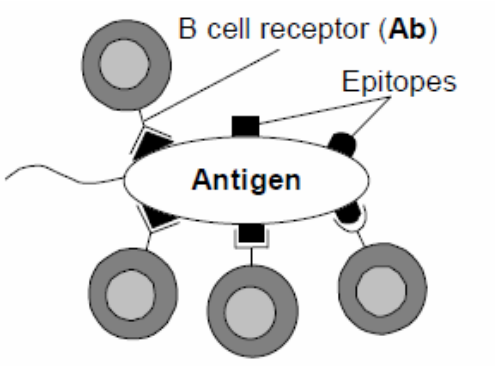


Figure 7: The Portion of an Antigen that is Recognized by an Antibody is called Epitope. Antigens may have Multiple Epitopes.

6.1 Antigen-Antibody Representations and Affinities

The Ag-Ab representation will partially determine which distance measure shall be used to calculate their degree of interaction (complementarily). Mathematically, the generalized shape of a molecule (*m*), either an antibody (**Ab**) or an antigen (**Ag**), can be represented by a set of real-valued coordinates $m = \langle m1, m2, ..., mL \rangle$, which can be regarded as a point in an *L*-dimensional real-valued space ($m \in SL \subseteq L$, where *S* represents the shape-space and *L* its dimension).

The affinity between an antigen and an antibody is related to their distance, that can be estimated via any distance measure between two strings (or vectors), for example the Euclidean or the Manhattan distance. In the case of Euclidean distance, if the coordinates of an antibody are given by <ab1, ab2, ..., abL> and the coordinates of an antigen are given by <ag1, ag2, ..., agL>, then the distance (D) between them is presented in Equation (1). Equation (2) depicts the Manhattan's distance case.

$$D = \sqrt{\sum_{i=1}^{L} (ab_i - ag_i)^2} \quad \ldots(1)$$

$$D = \sqrt{\sum_{i=1}^{L} |ab_i - ag_i|} \quad \ldots(2)$$

Shape-spaces that use real-valued coordinates and that measure distance in the form of Equation (1) are called *Euclidean shape-spaces*.

6.2 Real Value Representation

Our data consist of fields have different types characters and numbers. To unite them, we convert characters to numbers, and then applied normalization process on them to obtain values in range [0 – 1].

The benefit of data transformation such as normalization may improve the accuracy and efficiency of artificial algorithms. Such methods provide better results if data to be analyzed has been normalized, that is, scaled to specific range as [0 – 1].

- **Min-Max Normalization**: The min-Max normalization performs a linear transformation on the original data values. Suppose that minX and maxX are the minimum and maximum of feature X. In order to map interval [minX - maxX] into new interval [new minX – new maxX]. Consequently, every value v from the original interval will be mapped into value new_v by using Equation (3) [1]:

$$new_v = \frac{v - minX}{maxX - minX} \quad \ldots(3)$$

7. An Immune Complement Algorithm (ICA)

The classical pathway is evolution processes of complement molecules, in which, the complement molecules are cleaved respectively, then bind together and form a membrane attack complex, which can dissolve the plasma membrane.

In ICA, the plasma membrane, the complement and the affinities are the objective function, the feasible solution and the match degree between the solutions and the objective function, respectively, in later sections the ICA as in [3] with additional two steps NS and PS.

7.1 The Definition of Cleave Operator and Bind Operator

1. Cleave Operator O_C

A complement individual $a = (x_1, x_2, \Lambda, x_m)$, according to a cleaved probability, is cleaved in two sub-individuals: a_1 and a_2 .

$$O_C(a)=\begin{cases} a_1=P_c.a=(X_1, X_2,.., X_{Pc}) \quad aff(a_1) \geq aff(a_2) \\ a_2=(1-P_c).a=(X_{(Pc+1)},X_{(Pc+2)},..,X_m) \; aff(a_1) < aff(a_2) \end{cases} \quad \ldots(4)$$

Where P_c is the cleave probability, $aff(i)$ is the affinity of the complement individual i.

2. Bind Operator O_B :

Suppose there are two individuals: $a = (x_1,x_2, \Lambda, x_m)$ and $b = (y_1,y_2, \Lambda, y_n)$, there are two kinds of bind ways.

- **Positive bind operator** O_{PB} :

A new individual $c = O_{PB}(a,b) =(x_1,x_2,\Lambda,x_m,y_1,y_2, \Lambda, y_n)$ ...(5)

- **Reverse bind operator** O_{RB} :

A new individual $c= O_{RB}(b,a) = (y_1,y_2, \Lambda, y_n, x_1,x_2, \Lambda, x_m)$ ...(6)

7.2 The flow of ICA

ICA is composed of three phases: the identify phase, the active phase, the membrane attack phase. The flow of ICA is as follows, (see Figure 8),

Step1. Create an initial, random population of Complements detectors A_0 ($|A_0|= n$), from the training attack records and each one contains 41 real values.

Step2. Termination: apply Positive and Negative Selection, if the affinity of Euclidean distance between the current population of Complements detectors (CDs) and NonSelf (Ags), has contained the optimal individuals(match maximum attack records & not match maximum normal records) or achieved the maximum generation, then the course halts, else, continues.

Step3. Identify Phase:

Step3.1. Compute the affinity of each individual in $A0$;

Step3.2. Sort all the individuals CDs by their ascending affinities, then get $A_t= \{a_1, a_2, \Lambda, a_k\}$.

Step4. Active phase:

Divide At into $A_t^1= \{a_1, a_2, \Lambda, a_k\}$ and $A_t^2= \{a_{k+1}, a_{k+2}, \Lambda, a_n\}$, namely $At = A_t^1 \text{ Y } A_t^2$.

Where k is the Divide active variable, $A_t^1= \{a_1, a_2, \Lambda, a_k\}$ is a cleave set, $A_t^2= \{a_{k+1}, a_{k+2}, \Lambda, a_n\}$ is a bind set.

Step5. For each individual A_i ($i \in \{1,2,\ldots,K\}$) of A_t^1, execute $O_C(a_i)$ and get a remainder cleave set ($a_{1j}, a_{2j}, \Lambda, a_{kj}$)($j = \{1,2\}$), then execute $O_{PB}(a_{1j}, a_{2j}, \Lambda, a_{kj})$,finally get an individual bt .

Step6. Membrane attack process:

Step6.1. Bind b_t and each individual of A_t^2, namely

$O_{RB}(b_t, a_i)(i \in \{K + 1, K + 2, \Lambda, n\})$, then get a membrane attack complex set $C_t= \{c_1, c_2, \Lambda, c_{n-k}\}$ ($c_i = O_{RB}(b_t, a_i)$, $i \in \{1,2, \Lambda, n-k\}$);

Step6.2. For each c_i of C_t , recode it by the code length of initial individual, then gets a new set $C' = \{c'_1,c'_2, \Lambda , c'_{n-k}\}$.

Step7. Create a random population of complement individuals $D=\{d_1,d_2, \Lambda ,d_k\}$, then join them into $C' = \{c'_1,c'_2, \Lambda , c'_{n-k}\}$, finally form a new set
$E = C' Y D = \{ c'_1,c'_2, \Lambda , c'_{n-k}, d_1,d_2, \Lambda ,d_k\}$.
Step8. $t = t + 1$, Go to Step2
Step9. Positive Selection between the final Complement Detectors and NSL-KDD attack test records and compute the Detection Rate.
Step10. Negative Selection between the final Complement Detectors and NSL-KDD normal test records and compute the False Alarm Rate.

ICA has the following characters:
(i) It simulates the classical pathway of the complement system.
(ii)The cleave operator and bind operator can accelerate the convergence of the algorithm through selecting (PS & NS) and reserving the individual with high affinity in the next generation population.
(iii) There are little manual parameters, which make the algorithm executed automatically[3].

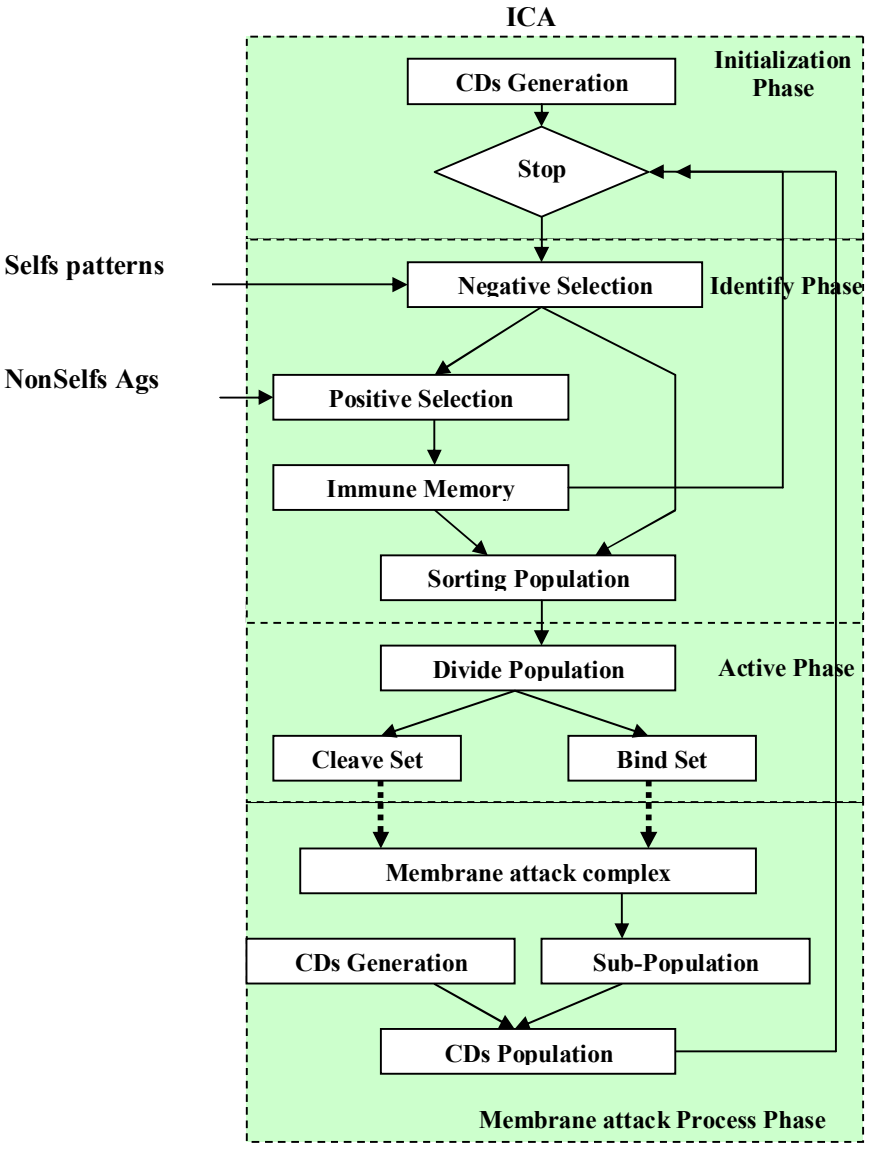


Figure 8: The overall diagram of ICA.

8. Performance Measurement

Detection Rate & False Alarm Rate: they ARE also called: sensitivity & specificity, true positive rate (TPR) & true negative rate (TNR). To get optimal balanced classification ability, sensitivity and specificity are usually adopted to monitor classification performance on two classes separately [2].

$$\text{True Negative Rate } (Acc^{-}) = \frac{TN}{TN+FP}$$

$$\text{True Positive Rate } (Acc^{+}) = \frac{TP}{TP+FN}$$

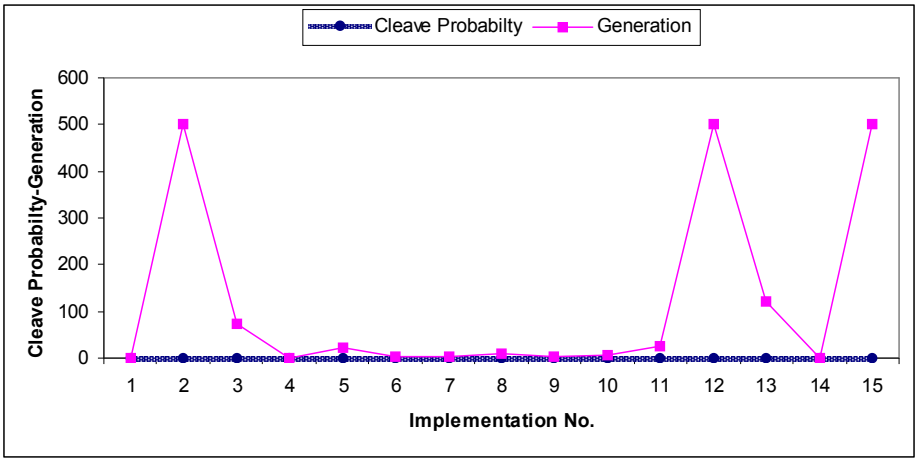
Where TN (true positive), attack records identified as attack; TN (true negative), normal records identified as normal; FP (false positive), normal records identified as attack; FN (false negative), attack records identified as normal [2].

9. Experimental Results

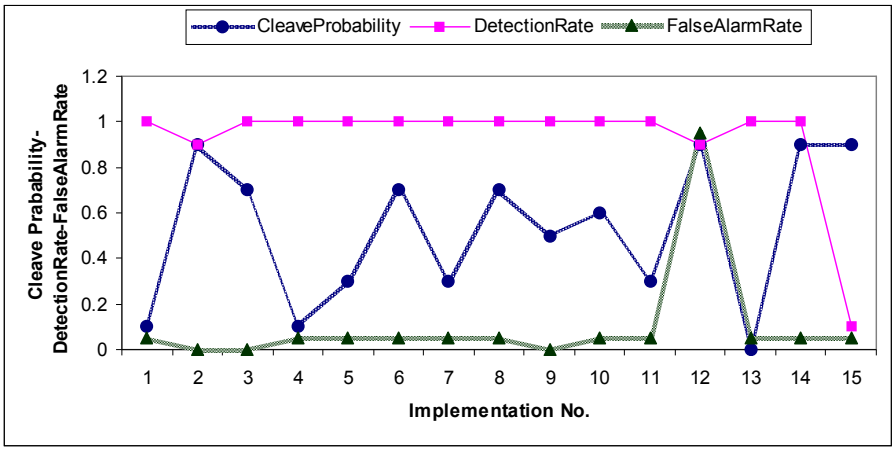
We use C# Language in applying this model, and the input parameters used for the experiments and their values are as the following:

- SelfNo: no. of normal NSL-KDD records.
- NonSelfNo(Ag): no. of attack NSL-KDD records separate for each type training and testing.
- Population size: 50 Complement Detectors.
- Maximum No of Generation: 500 .
- Divide active variable (k): is (10-95)% of Population size.
- Cleaved Probability: random value between [0-1].
- Threshold of Positive Selection = 0.01.
- Threshold of Negative Selection = 0.0001.

The thresholds used in the model were selected under too many experiments. ICA has almost times the optimal result; Detection Rate equal (1) and False alarm equal (0 or 0.05), from the Figure 9(a, b), we see the influence of Cleaved Probability on quicker the convergence when Divide active variable is 40% Population size. Also, the Divide active variable has approximation the same influence or little less on the results, see Figure 10(a, b) Cleaved Probability = 0.5.

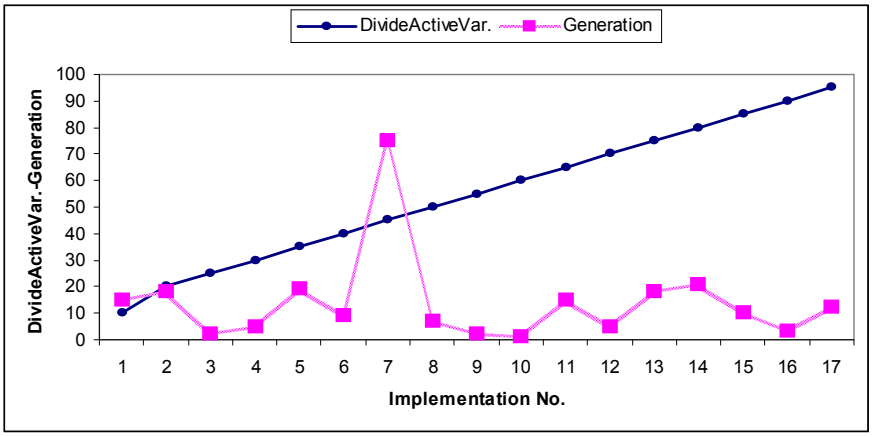


(a)

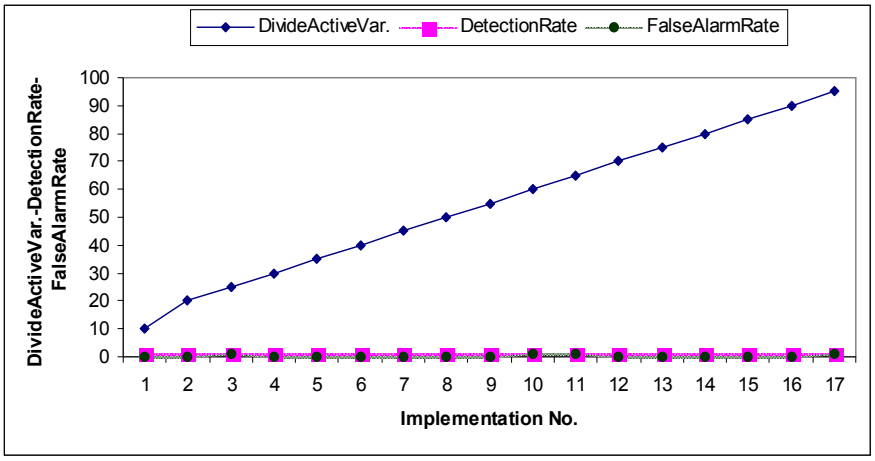


(b)

Figure 9: the Influence of Cleaved Probability on No of Generation (a), Detection Rate and False Alarm Rate(b), Divide Active Variable=40%.



(a)



(b)

Figure 10: the influence of Divide Active Variable on No of Generation (a), Detection Rate and False Alarm Rate(b), Cleaved Probability= 0.5.

10. Conclusions and Future Work

There is a whole and wide range of effectors mechanisms used by the immune system to eliminate foreign pathogens, or malfunctioning cells. Almost none of these processes have ever been model in AIS. For instance, those artificial immune systems used for anomaly detection and pattern recognition only incorporate immune metaphors for the detection of pattern (anomalous or not). Some of the mechanisms used by the IS to eliminate these detected patterns could be used as sources of inspiration for the development of computational strategies also capable of eliminating patterns in a computer system. It becomes from suitability to trend in the development of new AIS that refers to the modeling of other immune parts and processes and their application to problem solving.

Here and for future perspective, it is possible to add an antigenic recognition to classify the attack types, or it may be worthwhile to built a hierarchical multilayer defense system inspired from IS to detect intrusion.

REFERENCES

[1] Andries, P. Engelbrecht, "*Computational Intelligence An Introduction*", 2007.

[2] Chao Chen, Andy Liaw, and Leo Breiman, "*Using Random Forest to Learn Imbalanced Data*", Department of Statistics, UC Berkeley, 2004.

[3] Chen Guangzhu, Li Zhishu, Yuan Daohua, Nimazhaxi and Zhai yusheng. "*An Immune Algorithm based on the Complement Activation Pathway*", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.1A, January, 2006.

[4] Christoph Ehret, Ulrich Ultes-Nitsche. "*Immune System Based Intrusion Detection System*", Boulevard de Pérolles 90, CH-1700 Fribourg, Switzerland {christoph.ehret,uun}@unifr.ch

[5] Dipankar Dasgupta, "*Advances in Artificial Immune Systems*", IEEE Computational Intellegence Magazine, November 2006.

[6] Hongwei Mo, "*Handbook of Research on Artificial Immune Systems and Natural Computing: Applying Complex Adaptive Technologies*", Copyright © 2009 by IGI Global.

[7] http://nsl.cs.unb.ca/NSL-KDD/

[8] *Immunology*, exampille.com.

[9] Kasthurirangan Parthasarathy, "*Clonal Selection Method for Immuntiy based Intrusion Detection Systems*".

[10] L. N. de Castro and J. Timmis. "*Artificial Immune Systems: A New Computational Intelligence Approach*", Springer, 2002.

[11] Leandro Nunes de Castro, Fernando José Von Zuben. *"Artificial Immune Systems: Part I – Basic Theory And Applications*". Technical Report TR – DCA 01/99 December, 1999.

[12] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "*A Detailed Analysis of the KDD CUP 99 Data Set*", Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defence Applications (CISDA 2009).

[13] Stephanie Forrest and Catherine Beauchemin, "*Computer Immunology*". October 29, 2006.