ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

A New Approach on Intrusion Detection Based On Avidity Model Clonal Selection

N.Priya, Sundararajan.M, Arulselvi S

Assistant Professor, Ramanujam Centre For Computational Intelligence, Department of CSE, Bharath University, Chennai, India.

Director, Research Center for Computing and Communication, Bharath University, Chennai, India
Co-Director, Research Center for Computing and Communication, Bharath University, Chennai, India

ABSTRACT: To make an immune-inspired network intrusion detection system (IDS) effective, this paper proposes a new framework, which includes our avidity-model based clonal selection (AMCS) algorithm as core element. The AMCS algorithm uses an improved representation for antigens (corresponding to network access patterns) and detectors (corresponding to detection rules). In particular, a bio-inspired technique called gene expression programming (GEP) is integrated with artificial immune system (AIS) in detector representation. In addition, inspired by the avidity model of immunology, this paper also defines new avidity/affinity functions (corresponding to the metric for quantify the interactions between detector and antigens) that take the priorities of attribute into account. Accordingly, the proposed algorithm integrates both negative selection and positive selection with a balance factor k to assign appropriate weights to self and non-self avidity. The well known KDD CUP'99 DATA set is used for performance evaluation. The results show that the intrusion detection based on AMCS provides a higher detection rate of DoS attack, a lower false alarm rate, and a lower detectors generation cost. Our results indicate that breaking the bottleneck of immune-inspired network IDS through adjusting basic elements is feasible and effective.

KEYWORDS: network intrusion detection; artificial immune system; clonal selection; avidity model; gene expression programming

I. INTRODUCTION

The Internet is becoming the universal communication network for all kinds of information. It is envisaged to support not only current services, but also new services with varying traffic characteristics and quality of service (QoS) performance requirements [1]. Since network resources, such as buffer and link capacity, are finite and commonly shared by traffic flows, QoS is very sensitive to attacks, especially denial of service (DoS) attacks [2]. A DoS attack aims to deny access by legitimate users to shared services or resources. It can deplete the server system resources such as CPU and memory, use up the network resources, and disrupt the traffic transmission.

Network intrusion detection system (IDS) is one of general defense techniques against DoS attacks [3]. Although there has been a lot of research on intrusion detection, in order to more effectively cope with dynamic and increasingly complex networks, new direction based on computational intelligence approaches, e.g. artificial immune systems (AIS), is being pursued [4]. The immune-inspired IDS is based on AIS, which is an adaptive and computational system inspired by the principle and processes of biological immune system (BIS). In immune-inspired network IDS, a antigen corresponds to network access patterns, and a detector is the rule for recognizing attacks (intrusion or attack are used loosely).

Most of the existing immune-inspired IDS are based on negative selection (NS) algorithm. The first NS algorithm (NSA) and a network IDS architecture based on AIS called LYSIS were proposed by Forrest *et al*. [5]. Dasgupta and Zhou compared a negative characterization approach to positive characterization, and proposed an NS algorithm called *v*- detectors [6]. Kim and Bentley introduced a dynamic clonal selection algorithm (DynamiCS) which combined NS and clonal selection for network IDS [7]. Such approaches however have two major drawbacks, namely scalability and coverage, which have made immune-inspired IDS ineffective [4], [8]. Stibor *et al*. stated that NS is ***not*** appropriate for network IDS [9-10]. Nevertheless, Dasgupta believed that there are many aspects that are worth further exploration for NS algorithms [11].

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Fortunately, the algorithm inspired by clonal selection (CS) is more scalable than the NS algorithm. Based on the CS and affinity maturation theories, CLONALG algorithm is proposed [12], and the immune CS algorithm (ICSA) based structure is proposed for intrusion detection [13]. Recent research has also investigated the use of gene expression programming (GEP). A GEP-based constraint grammar and a constraint-based GEP rule extraction algorithm (CGREA) are proposed in [14]. We note that although with CGREA, the best rules are more effective than that of some methods based on other computational intelligence approaches, there are still some disadvantages of CGREA, e.g. the diversity of the generated rule population is still insufficient, and the coverage of many rules overlap with each other, resulting in a low efficiency.

To improve the existing immune-inspired network IDS, this paper proposes a new framework which consists of three modified basic elements: (1) detectors represented based on the constraint-based GEP, (2) avidity/affinity functions that consider attribute-priority, and (3) avidity-model based clonal selection (AMCS) algorithm, which is inspired by the CS and avidity model of BIS. Our work differs from the existing CS and NS algorithms by considering both NS and positive selection. Although our work uses CGREA to represent the detectors, it also has several novel aspects and critical improvement when compared to previous works on GEP.

The rest of the paper is organized as follows. In Section II, a new immune-inspired IDS framework, in which the AMCS algorithm is a critical component, is proposed to improve the detection performance and complexity. The experimental results are shown in Section III. Finally, Section IV concludes the paper.

II. FRAMEWORK BASED ON AVIDITY-MODEL BASED CLONAL SELECTION

In this section, we will first describe how to represent the antigens and detectors. We then define some avidity/affinity functions considering attribute-priority, and finally describe the proposed avidity-model based clonal selection (AMCS) algorithm.

A. Representation of Artificial Immune Entities

1) Antigen Representation

The proposed antigen genotype is shown in Fig. 1. The attribute set of antigen represents the abstraction of network behaviors. Each antigen is composed of n attribute genes, and classified as self and non-self (corresponding to network access pattern that is either normal or malicious).

***Definition* 1:** An antigen is denoted as follows:

$$I_{antigen} = \{(v_1, g_1), (v_2, g_2), \ldots, (v_n, g_n), category\}, \quad (1)$$

where (v_i, g_i) denotes the i-th (i=1, …, n) attribute gene, v_i and g_i is the ID and the value of the gene respectively, and category$\in$ {*self, non-self*}.

In this paper, the attributes of antigen correspond to the derived features of KDD CUP'99 DATA set (here in after to be referred as KDD'99 set), which can represent the interrelated network using the time-based traffic features. One KDD'99 set record and corresponding antigen are given below as Example1:

- Example1

KDD'99 connection record:
0,icmp,ecr_i,SF,132,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,511,511,
0.00,0.00,0.00,0.00,1.00,0.00,0.00,168,23,0.14,0.02,0.14,0.00,
0.00,0.00,0.00,0.00,smurf.
antigen:
{(a1,0),(a2,icmp),(a3,ecr_i),(a4,SF),(a5,132),(a6,0), … , (a23,
511), …, (a39, 0.00), (a40,0.00),(a41,0.00), ***non-self***}

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

In Example1, the attribute IDs (i.e. a1, a2, … , a41) correspond to the 41 features of KDD'99 connection records.

2) Detector representation

In this paper, a detector is represented differently from an antigen, and mainly includes the following fields:

a) Genotype ($\boldsymbol{I_{detector}}$), the encoding of a detector, which is composed of a set of genes. Each gene of a detector corresponds with one attribute of network behaviors.

b) Self avidity ($\boldsymbol{avidity_{self}}$), the value of binding strength with self antigens;

c) Non-self avidity ($\boldsymbol{avidity_{non\text{-}self}}$), the value of binding strength with non-self antigens.

The constraint-based GEP rule (here in after to be referred as GEP-rule), has been proposed in our previous research and been proved to be feasible and effective [14]. In this paper, we represent the detectors based on GEP-rule way, and give the following definitions for available individual of detector:

***Definition* 2:** Assuming that $I_{detector}$ consists of m attribute-judgment conditions, (v_i, f_i, b_i) denotes the i-th condition (i =1, … , m), v_i=index(a_i), $a_i \in$ attribute set A_s, $f_i \in$ function set F_s, and $b_i \in$ constant set C_s. then

$$I_{detector} = \{(v_1, f_1, b_1), (v_2, f_2, b_2), \ldots, (v_m, f_m, b_m)\}.$$

In $I_{detector}$, m is not larger than the number of attribute genes in antigen. However, different attribute-judgment conditions can use the same attribute ID.

A GEP-rule individual, its corresponding GEP-rule and detector are shown in Example2, which can recognized the antigen given in Example1.

- Example2

GEP individual: and. and. >=. >. <. a23. 10. a5. 3. a5. 300. a21
GEP-rule: (a5>3) and (a5<300) and (a23>=10)
detector: {(a5,>,3), (a5,<,300), (a23,>=,10)}

B. Avidity Function Based on Attribute Priority

According to the difference of affinity and avidity in the biologic **avidity model**, also known as quantitative model [15], in this section, we distinguish affinity and avidity in terms of numerical value via some definitions.

1) Affinity

If the attribute priority is considered when deciding whether each condition is matched, we can obtain a match degree as the affinity so as to realize not only the regular binary detector match, but also complete scale match and relationship match.

The attribute weight, says w, describes the importance degree of each characteristic attribute. The value of w can be a given constant or a value changed adaptively according to different task requirements.

***Definition* 3:** We use w_{bi} to denote the i-th attribute weight of detector b. w_{bi} has an alphabet of cardinality 3 with values: t_1, t_2 and t_3, while the i-th attribute is a core, important and assist attribute of b respectively.

In addition, we define a normalized match degree between detector b and antigen g based on distance function, denoted by M_{bg}, as follows. To ensuring the smaller distance reflects a better match, we assume that $t_1 < t_2 < t_3$, and let $max(w)$ denote the maximum value of w.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

$$M_{bg}(w) = \frac{\sum_{i=1}^{m} w_{bi}}{m \times max(w)}. \quad (2)$$

Based on the normalized match degree, we can define the affinity between a detector and an antigen, and the avidity between a detector and antigens as follows.

Definition* 4: *affinity, is 0 when detector does not match antigen; otherwise, their affinity is according to their distance. The affinity between detector *b* and antigen *g* is calculated as in (3).

$$affinity(b,g) = \begin{cases} 0 & ; \text{if none attribute value can be matched} \\ e^{-M_{bg}} & ; \text{others} \end{cases} \quad (3)$$

2) Avidity

Being different from affinity that means the similarity of the detected distance between detector and antigen, avidity is the objective function for the candidate solutions, or the metric for evaluating the adaptation of the candidate solutions.

Definition* 5: *avidity, reflects the interaction of one detector and all antigens, and is classified as self and non-self avidity.

Self avidity is the avidity between the detector and self antigens. Let *b* denote a detector, T_{Nb} is the number of self antigens recognized by *b*, and *N* is the original amount of self antigens, we define $avidity_{self}$ to be the self avidity of *b* and be calculated as in (4).

$$avidity_{self}(b) = \frac{T_{Nb}}{N} \quad (4)$$

Non-self avidity is the avidity between the detector and non- self antigens. Let *b* denote a detector, T_{Pb} is the number of non- self antigens detected by *b*, and *N* is the original amount of non- self antigens, we define $avidity_{non\text{-}self}$ to be the non-self avidity of *b* and be calculated as in (5).

$$avidity_{non-self}(b) = \frac{\sum_{i=1}^{N} affinity(b,g_i)}{T_{Pb}} \quad (5)$$

C. Avidity-Model based Clonal Selection Algorithm

A critical component in any immune-inspired IDS is the immune algorithm. Neither a negative selection (NS) algorithm nor an affinity only based clonal selection (CS) algorithm can realize more than one type classification.

In order to overcome the deficiencies of these existing approaches, we propose an improved immune algorithm: avidity-model based CS, called AMCS, based on the avidity model of immunology and CGREA. More specifically, we first discuss the value of avidity in (6) and then describe the proposed algorithm.

1) Avidity Calculation

A good detector should have a high non-self avidity and low self avidity. Therefore, we first define two functions: $f_{self}(b)$ and $f_{non\text{-}self}(b)$, where the former is the increasing function of $avidity_{self}$, and the latter is the decreasing function of $avidity_{non\text{-}self}$. They are calculated as follows:

$$f_{self}(b) = \exp\left(\frac{(avidity_{self}(b)-1)\times 10^{k}}{(10^{k}+1)}\right)$$

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

where k is a balance factor and used to balance the degree weights for self avidity and non-self avidity within the whole avidity. Then, we propose the following avidity function:

$$avidity(b) = f_{self}(b) \times f_{non-self}(b) . \quad (6)$$

2) Algorithm Description

The basic idea of the proposed AMCS algorithm is as follows. Initially, all detectors satisfying the constraint grammar G, which is defined in our previous works [14], are included. The detectors which have the lowest avidity in the historical sets are included to the optimal detector set.

The following is a list of notations used to describe the algorithm.

$S_{antigen}$: antigen set;
$S_{C\_detector}$ and $S_{best\_detector}$: the clone detector population and the optimal detector set, and their sizes are p_n and p_{best} respectively, where $p_{best} \leq p_n$;
g_e, g_m, g_{max}: the current evolution generation, the number of continuous non-upgraded generation and the maximum evolutional generation respectively;
p_1, p_2: The parent detectors of selection operation;
o_1, o_2: The offspring detectors generated by evolution operators (crossover and mutation).

Before executing the algorithm, we extract the antigens from the original data set, such as network packets, and log data, etc. These antigens, including self and non-self, are stored in $S_{antigen}$. The AMCS works as follows.

Algorithm: avidity-model based clonal selection (AMCS)

Input: $S_{antigen}$
Output: $S_{best\_detector}$

Step1: Generate the initial individuals of $S_{C\_detector}$ (the same as step 1 of CGREA);

Step2: Build $S_{best\_detector}$ and a temporary detector population $S_{tmp\_detector}$ with population size p_n ;

Step3: Submit each antigen of $S_{antigen}$ to $S_{C\_detector}$, calculate the $avidity(I_{detector\_i})$ according to (6), where $\forall I_{detector\_i} \in S_{C\_detector}$, i=1, …, p_n, and update $S_{best\_detector}$ in which the individuals are the best p_{best} ones in ($S_{C\_detector} \cup S_{best\_detector}$). If $S_{best\_detector}$ has not been upgraded during the g_m generations, go to Step 6;

Step4: Select two individuals, say p_1 and p_2, from $S_{C\_detector}$. Then execute the crossover operation and mutation operation, and generate o_1 and o_2 satisfied with the constraint grammar G;

Step5: Add o_1 and o_2 into $S_{tmp\_detector}$. If the population of $S_{tmp\_detector}$ is smaller than p_n, go to Step 4; otherwise $S_{C\_detector}$:= $S_{tmp\_detector}$; if the current evolution generation does not above the g_{max}, increase g_e by 1 and go to Step3 ;

Step6: Output $S_{best\_detector}$.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

II. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, we describe the experimental environment and parameter settings, and evaluate the proposed ACMS framework utilizing the well known KDD'99 set.

A. Environmen and Parameter Setting

The KDD'99 set has been recently utilized extensively for intrusion detection development and researching through a suite of bio-inspired computing algorithms. It provides two data sets, namely 10% Training Set and Test Set [16]. Each record is labeled as either normal, or as an attack. The attack records are grouped into one of the four categories: Probing, DoS, User to Root (U2R), and Remote to Local (R2L). The actual numbers of records in the data sets which are used in our experiments are listed in Table I. The records in the two subsets, namely Training subset and Test subset, are randomly sampled from the
10% Training Set.

Performance is measured in terms of detection rate p_d and false alarm rate p_f, estimated as follows:

the attribute set A_s is { $a1$, $a2$, … , $a41$} corresponding to the feature set for the KDD'99 records. The other GEP parameters are set as follows: size of optimal detector set p_{best} =20, crossover probability p_{cross} =0.2, mutation probability p_{mute} =0.95, length of head h=8, function symbols probability p_{func} =0.6, attribute symbols probability p_{attr} =0.28, and roulette wheel selection is conducted. To calculate the attribute weight and avidity, we set t_1=1, t_2=2, t_3=3, and balance factor k=2.

B. Results and Analysis

The proposed AMCS algorithm is executed for training using the Training subset, and tested on the 10% Training Set and the Test subset (Table I). Fig.2 summarizes the performance of 12 training runs. The false alarm rates from 24 detection tests (12 detectors sets test on two test sets) range from 0.1% to 0.5%. Tested on the 10% Training Set, the detection rates are mostly between 98.8% ~ 97.6%, which is much better than that of test subset. The results in Fig. 2 indicate that the optimal detector sets generated by AMCS can achieve a lower p_f and a consistent p_d. If the distribution of training set is the same as that of test set, the detection performance of the AMCS algorithm will be better.

Table II presents a comparison of detection performance between the AMCS algorithm and some other intelligent methods. In AMCS, the detector set that provides the best detection performance among the 12 sets in Fig.2, is selected for testing. As can be seen from Table II, although the attack detection rate achieved by AMCS is slightly lower than that of most other methods, but the false alarm rate is close to that of KDD'99 winner 1. The highest detection rate is obtained using Neural Networks, but with a very high false alarm rate (2.13%) compared to 0.51% obtained with the proposed AMCS.

In order to detect the 22 types of attack in the 10% Set and achieve the performance shown in Table II, AMCS merely used
20 (the size of optimal detector set) bi-attribute

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

$$p_f = F_P / N \quad , \tag{7}$$

where P and N are the total number of attack and Normal records in the test set. T_p and F_p are the number of attack and Normal records covered by given detector set.

In our implementation of the proposed AMCS framework, each detector is a single-gene GEP individual, in which the function set F_s is {and, or, not, >, ≥, <, ≤, =, !=}. In addition, each element of constant set C_s is random constant∈[0.1], and

Figure 2. AMCS algorithm performance of 12 runs

TABLE I. DISTRIBUTION OF TRAINING AND TEST DATA SETS

Category	10% Training Set	Training subset	Test Set	Test subset
Normal	97278	986	60593	4000
Probing	4107	41	4166	1107
DoS	391458	3961	229853	13715
U2R	52	1	228	52
R2L	1126	11	16189	1126
totoal	494021	5000	311029	20000

TABLE II. COMPARISON WITH OTHER INTELLIGENT METHODS

Method	Attacks p_d (%)	Attacks p_f (%)	DoS p_d (%)
AMCS	90.67	0.51	97.26
KDD winner 1[17]	91.00	0.50	97.10
KDD winner 2 [18]	91.30	0.58	97.47
Neural Networks[19]	92.61	2.13	97.00
Domain- aware GP [20]	92.50	1.35	96.00

TABLE III. AMCS VS. *V*-DETECTORS NS

Option	AMCS	*v-detectors* NS [6]
p_n	60	1000
g_{max}	50	1000
p_{best}	20	100 ~ 800
p_d (%)	98.96	83.92
p_f (%)	0.46	1.45

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

detectors. In comparison, other methods used more temporal and space resources. For example, KDD winner 1 contained
500 decision trees for 22 specific attack types [17], while KDD winner 2 used 218 and 755 decision trees for five categories and specific attack types respectively [18]. In addition, Neural Network assigned 125 input neurons and five output neurons[19], and domain-aware GP used 100 detectors, which individual length is between 30~350, to detect five categories records[20].

The above discussion indicates that the AMCS algorithm can generate optimal detector set which can achieve a low false alarm rate and a high DoS attack detection rate with less time in detector generation and attack detection.

We have also compared AMCS with *v*-detectors, one of the main and best NS algorithms, using the same 10% Training Set. Since the training results of immune algorithms like these are stochastic and mostly depend on the parameter setting. We use the best result of *v*-detectors NS algorithm presented in the literature. The results are shown in Table III. These results show that even with a small population size p_n, a smaller max evolution generation $g_{\max}$, and a smaller size of optimal detector set p_{best}, which translates to a lower time and space complexity, the detectors generated by the AMCS algorithm can achieve a better detection performance.

IV. CONCLUSIONS

While the poor performance of prior approaches based on immune-inspired IDS has led to concerns about the viability of such approaches, we believe that immune-inspired IDS is still promising as it considers not only how to generate the detectors/rules for intrusion detection, but also how to build a complete security system for networks.

In this paper, we have proposed and demonstrated the applicability of improved novel framework, which integrates two biologically inspired computing techniques: AIS and GEP, for network IDS. The proposed framework overcomes two major problems of the existing immune-inspired network IDS, namely scalability and coverage. The experiment results have shown that the immune-inspired network intrusion detection based on the proposed framework provides a higher detection probability of DoS attacks, a lower false alarm rate and a lower detectors generation cost.

Even though is the proposed approach performance only slightly better than some of the other computational intelligence approaches, and certainly further improvement can be made, an important conclusion that can be drawn from this study is that breaking the bottleneck of immune-inspired network IDS through adjusting basic elements is feasible and effective.

REFERENCES

[1] H. Jonathan Chao, Quality of service control in high-speed networks, John Wiley & Sons, Inc. 2002.
[2] Hariharan V.S., Nandlal B., Srilatha K.T., "Efficacy of various root canal irrigants on removal of smear layer in the primary root canals after hand instrumentation: A scanning electron microscopy study", Journal of Indian Society of Pedodontics and Preventive Dentistry, ISSN : 0970-4388, 28(4) (2010) pp.271-277.
[3] P. Owezarski, "On the impact of DoS attacks on Internet traffic characteristics and QoS," in Proc. of 14th International Conference on Computer Communications and Networks (ICCCN 2005), San Diego, California USA, Oct. 2005, pp.269-274.
[4] Kanniga E., Selvaramarathnam K., Sundararajan M., "Embedded control using mems sensor with voice command and CCTV camera", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp.4794-4796.
[5] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Computing Surveys, vol. 39, no. 1, article 3, pp.1-42, April 2007.
[6] Das M.P., Jeyanthi Rebecca L., Sharmila S., "Evaluation of antibacterial and antifungal efficacy of Wedelia chinensis leaf extracts", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) pp.265-269.
[7] J. Kim, P. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, and J. Twycross, "Immune system approaches to intrusion detection - a review," Natural Computing, vol. 6, no. 4, pp.413-466, Dec. 2007.
[8] Subhashini V., Ponnusamy S., Muthamizhchelvan C., "Growth and characterization of novel organic optical crystal: Anilinium d-tartrate (ADT)", Spectrochimica Acta - Part A: Molecular and Biomolecular Spectroscopy, ISSN : 1386-1425, 87() (2012) pp.265-272.
[9] S. A. Hofmeyr, and S. Forrest, "Architecture for an artificial immune system," Evolutionary Computation, vol.8, no.4, pp.443-473, Dec. 2000.
[10] Thomas J., Ragavi B.S., Raneesha P.K., Ahmed N.A., Cynthia S., Manoharan D., Manoharan R., "Hallermann-Streiff syndrome", Indian Journal of Dermatology, ISSN : 0019-5154, 58(5) (2013) pp.383-384.
[11] Z. Ji, and D. Dasgupta, "Applicability issues of the real-valued negative selection algorithms," in Proc. of CEC 2003, Canberra, Australia, ACM, Dec. 2003, pp.111-118.
[12] J. Kim and P. Bentley, "Immune memory and gene library evolution in the dynamical colonal selection algorithm," Journal of Genetic

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Programming and Evolvable Machines, vol. 5, no. 4, pp. 361-391, Sep. 2004.

[13] E. Hart and J. Timmis, Application areas of AIS: The past, the present and the future, Applied Soft Computing, vol 8, issue 1, pp. 191-201, Jan.2008.

[14] T. Stibor, "On the appropriateness of negative selection for anomaly detection and network intrusion detection," Darmstadt University of technology, Germany, Ph. D thesis, 2006.

[15] T. Stibor, J. Timmis, and C. Eckert, "On the appropriateness of negative selection defined over hamming shape-space as a network intrusion detection system," in Proc. of CEC 2005, Edinburgh, UK, IEEE Press., July 2005, pp.995-1002.

[16] D. Dasgupta, "Advances in artificial immune systems," IEEE Computational Intelligence Magazine, vol. 1, no. 4, pp.40-49, Nov. 2006.

[17] L. N. de Castro and F. J. V. Zuben, "The clonal selcetion algorithm with engineering applications," in Proc. of GECCO 2000, Las Vegas, Nevada, USA, July 2000, pp.36-39.

[18] F. Liu and L Luo, "Immune Clonal Selection Wavelet Network Based Intrusion Detection,"in Proc. of Artificial Neural Networks: Biological Inspirations(ICANN2005),LNCS, vol 3696, Springer, 2005, pp.331-336.

[19] W. Tang, Y. Cao, X. M. Yang, and W. H. So, "Study on adaptive intrusion detection engine based on gene expression programming rules," in Proc. of International Conference on Computer Science and Software Engineering (CSSE 2008), Dec. 2008, pp.959-963.

[20] S. Mariathasan, R. G. Jones, and P. S. Ohashi, "Signals involved in thymocyte positive and negative selection," Seminars in Immunology. vol. 11, pp. 263-272, Aug. 1999.

[21] KDD CUP'99 DATA Set, http://kdd.ics.uci.edu/data bases/kddcup99/kddcup99.html

[22] C. Elkan, "Results of the KDD'99 Classifier Learnin", ACM SIGKDD 2000, Boston, MA, USA, Aug. 2000, vol.1, no. 2, pp.63-64.

[23] I. Levin, "KDD99 classifier learning contest LLsoft's results overview", ACM SIGKDD 2000, Boston, MA, USA, Aug. 2000, vol.1, no. 2, pp. 67-75.

[24] Y. Bouzida, and F. Cuppens, "Neural networks vs. decision trees for intrusion detection," in Proc. of IEEE / IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM), Tuebingen, Germany. Sep. 2006, pp.81-88.

[25] K. Faraun and A. Boukelif, "Genetic programming approach for multi- category pattern classification applied to network intrusions detection," International Arab Journal of Information Technology, vol.4, no.3, pp.237-246, July 2007.

[26] Bharthvajan R, Change Management - Models and Process, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 315-320, Vol. 2, Issue 1, January 2013

[27] Bharthvajan R, Performance Management & Appraisal System in an Organization, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 7192-7195, Vol. 2, Issue 12, December 2013

[28] Bharthvajan R, Marketing Research and Strategy-Down turn of Economy, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 5321-5324, Vol. 2, Issue 10, October 2013

[29] Bharthvajan R, Exit Interviews, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 12073-12076, Vol. 3, Issue 5, May 2014

[30] Bharthvajan R, ENTREPRENEURSHIP IN GLOBALISING ECONOMY IN ACCORDANCE WITH CAR INDUSTRY, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 14359-14361 Vol. 3, Issue 7, July 2014

[31] Bharthvajan R, Evaluation of Training and Development Programme, International Journal of Innovative Research in Science, Engineering and Technology, ISSN: 2319-8753,pp 13374-13377, Vol. 3, Issue 6, June 2014