A Novel Immunity Inspired Approach for Anomaly Detection

Praneet Saurabh
Deptt. of CSE, TIT
Bhopal, M.P, India

Bhupendra Verma
Deptt. of CSE, TIT (E)
Bhopal, M.P, India

ABSTRACT
Artificial Immune System (AIS) over the years has caught attention of researchers of various domains for complex problem solving. AIS model the procedure and methodologies of Biological Immune System (BIS) which protects the body from diverse attacks and different challenges. Scientists over the years are amazed with the appealing features of BIS that can be exploited. The most significant of them is its ability to distinguish self and non-self. This theory forms the basis of Negative Selection Algorithm (NSA) in AIS. NSA is competent for anomaly detection problems. From this perspective this research paper presents a Novel Immunity inspired approach for Anomaly Detection (NIIAD) with the feature of fine tuning. The main intention of adopting finetuning is to covering more self region and identifying non self region proficiently. Experimental results reflects high detection ratio with less false alarm and low overhead.

Keywords
Artificial Immune System, Biological Immune System, Negative Selection Algorithm, Anomaly, Fine Tuning

1. INTRODUCTION
Artificial immune system (AIS) is recognized as a new realm and is in a lot of focus [3]. Inspired by biologically immune system (BIS) AIS has now become sought after paradigm for complex problem solving in the domain of computational intelligence [14]. AIS mold various complex principles and processes of BIS which enables the all organisms to survive from the various threats and challenges. Reaction and response of BIS against these different and new threats and attacks persuade researchers to model computer security system after BIS, because it survives under very demanding circumstances very efficiently and effectively.

AIS covers all the methods and the subsequent efforts in the genre of computational models inspired by biological immune systems. Applications of AIS include anomaly detection, fault diagnosis, computer security, and optimization [12]. Out of the various mechanisms of biological immune system (BIS) that are modeled for AIS, Negative Selection is the most talked about models [4]. Forrest et al. [15] introduced negative selection algorithm (NSA) which distinguishes self and non-self. Inspired by the negative selection of T-cells in the thymus, it revolves around the immune system's ability to identify unknown antigens/ non-self while not reacting to the self-cells. NSA has been widely used in anomaly detection problems [7] and shown quite efficient to these problems. Due to these features of NSA over the years it has attracted the attention of many researchers which led to various versions of NSA.

Computer Security has emerged as the key challenge as pervasiveness of computers is now in every aspect and vertical of life [2]. The spirit of network and computer security is to keep the recourses, secure from non-intended recipients, preserve its integrity and availability at the same time. This pervasiveness, importance and value attached lures hackers to take advantage of the vulnerabilities [11]. Over the years a whole array of tools are developed and deployed to eliminate the threat perception but it is still there. Attack content and its methodologies have evolved and become more complex and very difficult to recognize the anomalous behavior.

In the currently prevailing scenario technology and biological systems has bidirectional relation and both benefit from each other [13, 17]. In this regard AIS possess many features can be explored in the context of anomaly detection. NSA has shown to be efficient for anomaly detection problems. In NSA detector exposure of self and non self is an important issue in identifying normal and attack. Many different variations in NSA tried to optimize but still it needs to be realized properly. This paper presents A novel immunity inspired approach for Anomaly Detection (NIIAD) which uses Enhanced Real Valued Negative Selection Algorithm (E-RNS). E-RNS incorporates finetuning to increase detector coverage of self and non-self. E-RNS is used to perform anomaly detection to identify unseen and novel attacks which are hard to detect.

Section 2 highlights related work of computer security with available tools and opinion of AIS in the canvas of computer security. Section 3 presents the Enhanced Real Valued Negative Selection Algorithm (E-RNS) to develop A novel immunity inspired approach for Anomaly Detection (NIIAD), experimental result and analysis is covered in Section 4 and Section 5 concludes this paper.

2. RELATED WORK
The nature of threat/ attack has changed over the years and it has become more severe. It is constantly evolving and increase in its number very clearly highlights this.

2.1. Types of Attacks
Attacks and intrusions identified at the user level by Harmer *et al.*[12] are as:

1. **Misuse/abuse:** unauthorized activities by authorized users.
2. **Reconnaissance:** findings of systems and services that may be **e**xploitable.
3. **Penetration:** successful access to computing resources by unauthorized users.
4. **Trojanization:** presence and activity of unauthorized processes.
5. **Denial of service:** an attack that obstructs legitimate access to computing.

Pervasiveness of internet, availability and access of to attack knowledge and methods have contributed in sharp rise of

internet attacks. Annual internet attack cases are increasing to a great extent have became new potential weapon of world war.

2.2. Firewall

Firewalls are first-line of defense for any network, it sits inline and is responsible to permit, deny or proxy data to a computer network. Firewalls are not always effective against the numerous intrusion attempts. Since the Firewalls are deployed for a network which monitors the incoming traffic to the network but it fails to addresses the attacks which comes or launched from within the organization. It also does not have a proactive approach to counter any new threat.

2.3. Intrusion Detection System

Intrusion Detection System (IDS) is a very important tool in the domain of computer security. It is based on identification of what is not legitimate and has deviation from the normal to be legitimate. Formally Denning defined it as the processes, and methods in order to facilitate identification, assess, and report unauthorized network activity [1, 2]. It works on the principle that the action and behavior of intruder will be different from that of a legitimate user. This collected information is matched and analyzed with any of the traditional statistical/ characteristics/ neural network/ data mining techniques to identify the threat or intrusion signatures [1, 5]. On the basis of basic detection techniques IDS are classified into **Misuse Detection** also called Rule-Based Detection or signature detection technique. This technique is based on the collected attack patterns (or "signatures") and then matched against the audit data stream. **Anomaly Detection** is also referred as profile-based detection; the main conjecture of anomaly detection is that pattern of attacks will be different from normal behavior.

Intrusion detection systems have their own restrictions, existing IDS are based on collecting, analyzing and extracting evidences after an attack which make it slow for reaction and often fail to give fitting response to the escalating number of new network attacks. Lack of self-learning and self-adapting abilities makes it even worse. This results in failure in detection and prevention of unknown network intrusions. Furthermore abnormal samples are not available at the training stage. An ideal solution needs to be resilient with self-learning and self-adapting abilities.

2.4. Biological Immune System

Biological Immune System (BIS) is constituted by central lymphoid with an objective to generate and mature immune cells called lymphocytes. These are continuously generated by bone marrow and mature in thymus. Thymus releases only the matured and beneficial T-cells to the blood stream and discards the remaining ones. Matured T-cells behave in the manner of a detector and identifies the invading antigens and takes suitable and appropriate measures [3]. Based on operation and reaction of Immune system it can be divided into two categories such as **Innate Immune System** represent**s** the defense mechanisms with which an individual is born, which provide security cover against foreign pathogens. Next is **Adaptive Immune System,** it is also termed as acquired immunity because it builds a memory over a period of time to achieve a faster response when the same threat or antigen is confronted next time. It acts as a supplement to innate immunity [4].

2.5. Artificial Immune System

Artificial immune system (AIS) entices researchers with its attractive qualities such as self-configuration, self-learning, self-adaptation, and distributed coordinating. The most prominent functionality is its ability to distinguish self and non-self. A lot of research and landmarks has been achieved since Jerne introduced it. New AIS models have been proposed time and again to solve different kinds of problems from the domain of computer security, data mining, clustering, data analysis, and classification.

2.6. Negative Selection Algorithm

Negative Selection Algorithm (NSA) was proposed by Forrest and her group in 1994 [15]. Inspired by natural immunity it revolves around the idea of negative selection of T-cells in the thymus. Principally it roams around the concept of immune system's ability to identify unknown antigens/ non-self while not reacting to self-cells. In the same way NSA first builds self profile, by recognizing normal network patterns as self and other patterns as non-self. With reference to this built profile the non self patterns are very easily identified and marked as non-self/ anomalous illustrated in Fig.1 & 2. Later on different variations in negative selection algorithms have been introduced [16, 23] but the core remained the same.

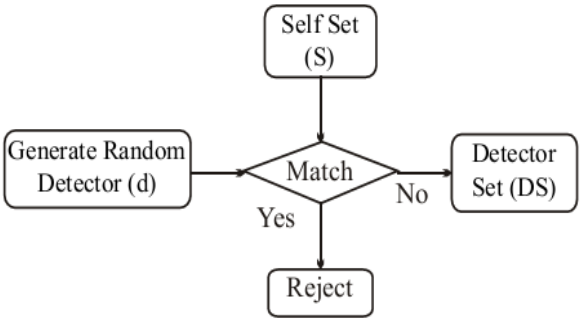

Fig.1 Detector Generation & Selection

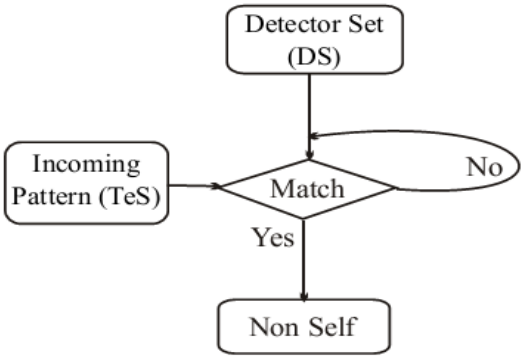

Fig.2 Non Self Detection

Negative Selection Algorithm (NSA) is represented through different methods. Binary representation and Real valued representations are the prominent ones. Binary representation present the problem in a finite problem space which is easier to analyze, and straightforward for categorized data [6]. However it also has several limitations such as lack of scalability and limited information extraction, which prevents it to be used more extensively. Gonzalez and Dasgupta [7] bring in real valued negative selection (RNS) algorithm to alleviate inadequacy of binary representation. Unfortunately, these randomly generated detectors still fall short in covering the non-self region in the most efficient way.

2.7. NSA and Anomaly Detection

Astonishing similarity exists between the requirements in the field of anomaly detection in computer security and the features offered by NSA inspired by biologicial immune systems [13, 14]. The most prominent one includes the mechanism that keeps the system stable in a highly dynamic and changing environment. The way BIS reacts and give response against different and new threats and attacks encourages and forms the base for the researchers to model anomaly detection in computer security system after Biological Immune System [16]. Similar to an organism which survives under very demanding circumstances very efficiently and effectively computer networks are also exposed to an array of attacks. AIS use these theories to develop algorithms which help in developing appropriate applications to solve different problems in the domain of computer security. The immunological inspired techniques are quite successful in anomaly detection [15, 19]. Anomaly detection aims to detect the abnormal behaviour of system that violates the established policy.

3. A NOVEL IMMUNITY INSPIRED APPROACH FOR ANOMALY DETECTION (NIIAD)

This section presents A Novel Immunity Inspired Approach for Anomaly Detection (NIIAD) which uses Enhanced Negative selection algorithm (E-RNS). E-RNS forms the base for NIIAD with fine tuning to cover more self non-self space. This enables NIIAD to efficiently detect known and unknown attacks.

3.1. Enhanced Real Valued Negative Selection Algorithm (E-RNS)

Fine tuning mechanism is introduced in Enhanced Real Valued Negative Selection Algorithm (E-RNS). Finetuning enables the detectors to efficiently and correctly cover more self non-self space. Detector coverage is an optimization problem and many works have focused on it. However it still remains a challenge to be realized efficiently and correctly [10].

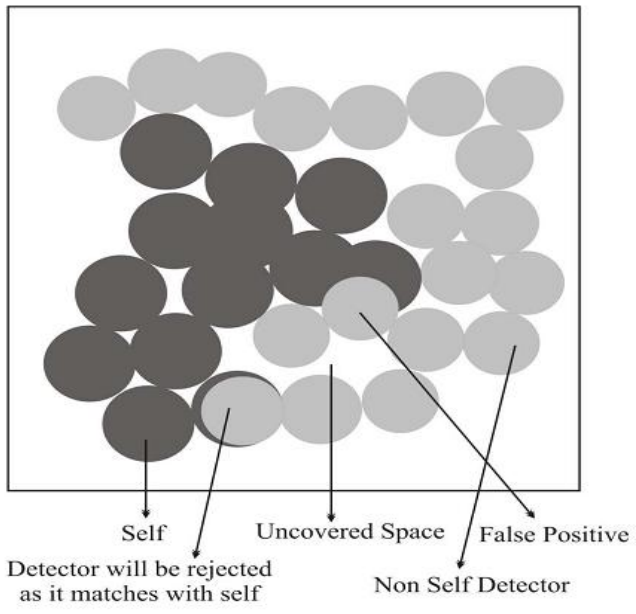

Fig. 3 NSA with constant detectors

Previous works have generated detectors of small or of the same size to cover self/ non-self space due to this some of self/ non-self space is not covered or covered with holes represented in Fig. 3, it is also called problem of similarity. Due to these methods and representations NSA fails to proficiently recognize self and non self space correctly. Enhanced Real Valued Negative Selection Algorithm (E-RNS) introduces self tuning (fig 4) which enables the detectors to cover the self and non self space efficiently and correctly. E-RNS uses real value random number generator to generate unique dissimilar random numbers to generate detector *(d)* in the Detector generation stage. This non similar value of detectors overcomes problem of similarity. At the next step of detector selection, detector *(d)* is compared with the instances of *Test Set* (*TS*). If the difference between detector *(d)* and Training Set '*TS*' is less than Binding Threshold (*B_T*) given by:

$$D(dx_i, TSy_i) < B\_T \qquad \text{-----(I)}$$

If equation *(I)* is true then detector *(d)* is not discarded which is used to happen in the previous works. In the proposed work this detector is finetuned and made dissimilar so that it is selected.

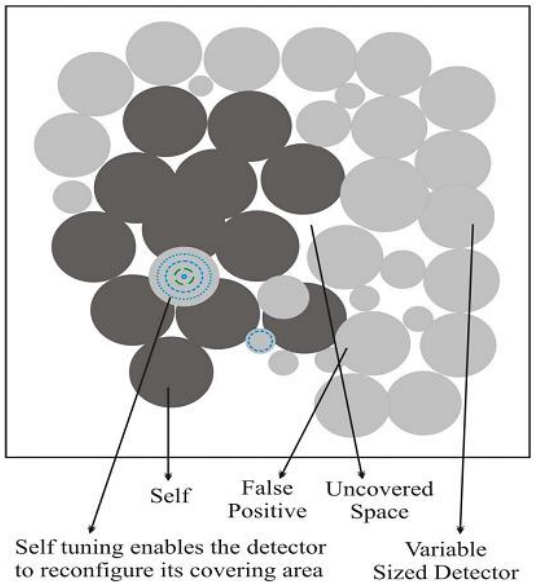

Fig. 4 E-RNS with variable detectors and selftuning

E-RNS incorporates self tuning with a tuning factor represented as (T_V) in this stage to make detector dissimilar. Detector *(d)* is altered by a factor of *'V'*, with this iterative alterations detector *(d)* becomes unlike and $D(dx_i, TSy_i) < B\_T$ becomes false. Once this detector becomes dissimilar then it is selected. Self tuning depicted in Fig. 4 makes a detector to cover as much correct space as possible. This reduces false positives and also the computational complexity required to generate and select detectors. Finetuning makes detector selection more efficient. It allows them to cover more self and non-self space correctly and minimizes computational cost.

3.2. A Novel Immunity Inspired Approach for Anomaly Detection

This section details the different phases of A Novel Immunity Inspired Approach for Anomaly Detection (NIIAD) including E-RNS which forms the heart of scheme.

3.2.1. Training Phase

Training phase has the task of generating and selecting competent detectors. Detectors coverage of self and non-self is

the prime objective of this phase. In the first step Real value random number generator is used to generate unique dissimilar random numbers within a specified range [0.0-1.0]. A detector in NIIAD represents any value in the shape space. Non similar values by real value random number generator helps in achieving uniqueness of the detector and also overcomes the problems of similar detectors highlighted in Fig 3.

In the next step detectors are selected from the generated ones. This phase uses the Enhanced Real Valued Negative Selection Algorithm (E-RNS) to select the best finetuned detectors in the problem space and then assign these detectors to identify and classify new (unseen) data as self or non-self. These detectors are used to detect anomalies. Detector *(d)* is matched with every instance of *Training Set* (*TS*). Different matching rules are there to do this comparison. Hamming distance and R-chunks, is used for binary representation, e.g. rcb (r-contiguous bit) [5, 15]. Euclidean distance is primarily used for matching in real-valued representation. It aims to find the distance between a data point and some detector lies within a certain threshold or not.

$$D(dx_i, TSy_i = \sqrt{\sum_i (dx_i, TSy_i)^2} = \|x_i, y_i\| \qquad \text{------ (II)}$$

makes detector *(d)* adapt and self configure itself dynamically. Different values of (*d)* also enable the detectors to cover up the uncovered space and holes in state space representation.

3.2.2. Testing phase

In this phase each detector *'d'* is compared to all the instances of Test Set *(TeS)*. Euclidean similarity measure is calculated between detector *(d)* and *1* to k^{th} element of *TeS*. If the similarity measure is greater than *A_T (Affinity_Threshold*), predefined threshold, then the test sample is labeled as an anomaly. Older detectors are replaced when its *Risk_Count* becomes greater with the new cloned detectors who are more proficient and have updated information. This mechanism helps in detecting the new attacks and achieving higher detection rate.

1. Input: *RS* = Rule Set
2. Input: *d*= Detector
3. Input: *TeS*= Test Set
4. Input: *A_T*= Affinity Threshold=0
5. ASSIGN *d* and *RS*
6. for all d(*RS*) $_{1 \text{ to k}}$ for all packets in *TeS* $_{1 \text{ to k}}$
7. if $D(dx_i, TeSy_i) > A\_T$
8. ANOMALY
9. else
10. NORMAL
11. end if
12. end for

4. EXPERIMENTAL RESULTS AND ANALYSIS

This section discusses the performance of proposed NIIADS, and its potential advantages over RNS with constant detectors.

4.1. Dataset

All the experiments in this paper are carried on KDD Cup 99 dataset. KDD Cup 99 dataset is most common, widely acceptable and recognized dataset [8]. It is still used extensively as standard dataset for anomaly detection in computer security problem. Various researchers [18, 20] used it to train, test and verify their findings. It is derived from the DARPA IDS evaluation dataset [21, 22]. The complete dataset have about 5 million records and each record represents a TCP/IP connection that is composed of 41 features which are both qualitative and quantitative in nature plus a label of either "normal" or "attack."Training dataset contains only normal records of KDD cup 99 dataset but each record has 33 numerical features, this large number of dimensions makes computation very complex and time consuming. NIIAD uses Principal Component Analysis (PCA) with Min Max Normalization in order to prevail over this challenge of dimensionality.

Principal Component Analysis (PCA) is very common feature selection approach. It identifies and selects important and relevant features while leaving the irrelevant ones [20]. It yields the most significant Principal Components called the network features (f_1, f_2,……f_5). Min-Max Normalization is used to normalize the principal components network features (f_1, f_2,……f_5) in the range [0, 1] from the range of (-32322 to 54334). Now in the present scenario it would have taken much computational time and processing. PCA with Min Max Normalization make the dataset computationally relevant and system powerful, stable. Pre-processing configuration is saved for applying on test data.

4.2. Experimental Setup

Both the methods RNS and NIIAD use KDD Cup dataset for training and testing purposes and then comparisons have been drawn. Attack free data is used in training and attack included samples is used for testing. In the training set, 972,781 records are normal and the rest is attack traffic. In all the experiments test set is composed of 5000 randomly selected unseen data, which includes both normal and attack. All the results are the average of 50 runs on the same configuration. Detection Rate and False Alarm are the two parameters that define the efficiency of detection system. Detection rate represents the percentage of identified anomalies. False alarm rate illustrates of the detection system generates an alarm in normal conditions. High detection rate and low false alarm rate are prerequisites for any detection system. Following measures are used to compute the performance of the NIIAD [18].

(i) Detection Rate (DR): $\frac{TP}{TP+FN} * 100$

(ii) False alarm rate (FAR): $\frac{FP}{TN+FP} * 100$

4.2.1.Detector Selection ratio with Training data size

This experiment is carried with the intension to identify the difference which fine tuning makes in detector selection.

Table. 1

Training Data	Method	Detector Selection (%)	Detector Rejection (%)
25%	RNS	77.38	22.62
	NIIAD	97.15	2.85
50%	RNS	43.3	56.7
	NIIAD	99.1	0.9
100%	RNS	17.26	82.74
	NIIAD	99.9	0.1

Table 1 illustrates the effect of finetuning in selection of detectors. These results are an average of 50 runs of different number of detector generation while tuning factor (T_V) remains as 1. Detectors are generated with variation in the training sample size of preprocessed data by using both RNS and the proposed NIIAD. The results in table 1 very clearly reflect that the selection percentage of detectors by using the proposed NIIAD is much higher than RNS. As the training data increases from 25% to 100 % then difference in selection percentage of RNS and NIIAD increases very sharply because larger amount of self helps in creating self profile efficiently. Finetuning introduced in detector selection aids this high selection percentage as detectors are nor discarded after just one comparison but it is tuned so that it become non similar. As the training samples increases the selection percentage of detectors in RNS comes down and detector rejection percentage increases since RNS discards a detector just after one failed comparison. As a result it has to generate more detectors to map the whole self sample.

4.2.2. Detection Rate and False Alarm Rate

This experiment has the objective to identify and compare detection rate and false positive rate of both the methods RNS and E-RNS with variation in training data. Table 2 illustrates the effect of training samples in detection when it is varied from 25% to 100%. Same training data and test set is used. Affinity threshold remains 0.4 and against variation in training sample the relative average detection rate and false alarm of RNS and NIIAD is calculated.

From the observations illustrated in table 2 it can be easily quantified that the proposed NIIAD achieves higher detection rate and lower FAR than RNS. Lower value of self samples for training indicates that limited information is available to generate the self space. However NIIAD successfully creates the full profile and achieves better results while maintaining stability. In some cases RNS fails to maintain stability in the results and FAR becomes 100%. NIIAD successfully generates self profile and achieves 100% detection while FAR also remains at the lower side.

Table. 2

Training Data	Method	Detection Rate	False Positive Rate
25%	RNS	100	100
	NIIAD	100	0.8
50%	RNS	100	1.12
	NIIAD	100	0.71
100%	RNS	91.7	0.72
	NIIAD	100	0.70

4.2.3.Affinity Threshold vs Detection Rate and False Alarm Rate

This result demonstrates the importance of affinity threshold used for identifying an anomaly in the test set. Selected Detectors are compared with the instances of test set. Detectors used in this experiment are trained with 100% of the samples while test set remains same for all the experiments. Observations in Table 3 points out that as the affinity threshold increases from 0.2 to 0.4 the detection rate of NIID increases and FAR comes down when compared to RNS. FAR of RNS increases in some instances which is never desired.

Table. 3

Affinity Threshold	Method	Detection Rate (%)	False Positive Rate (%)
0.2	RNS	88.62	0.62
0.2	NIIAD	89.89	0.62
0.3	RNS	90.5	0.71
0.3	NIIAD	92.9	0.68
0.4	RNS	91.7	0.72
0.4	NIIAD	100	0.70

Fig. 5 reflects the detection rate and false alarm rate of RNS and NIIAD when measured under different affinity thresholds from 0.2 to 0.4 with 20 variations. Detection Rate of RNS remains lower to the curve of NIIAD in all the variation in the affinity threshold. Also FAR of RNS is higher when compared to curve of NIIAD.

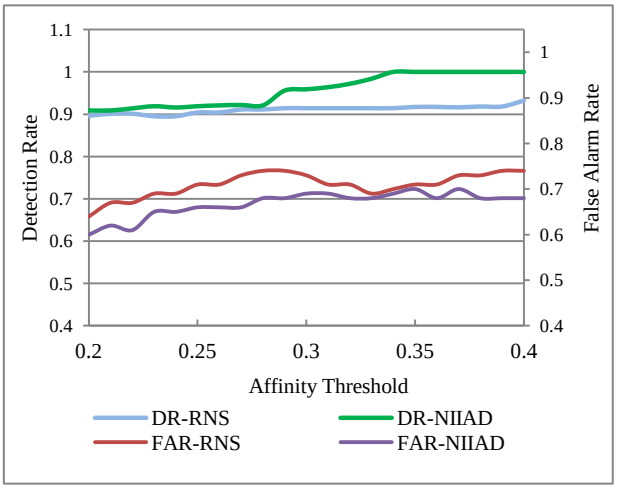

Fig. 5 Affinity Threshold vs Detection Rate vs FAR

It clearly indicates that under all the values and test condition NIIAD attains better results and achieves a Detection Rate of 100%, with only 0.70% false alarm rate in the best case.

5. CONCLUSION

This paper presents NIIAD inspired by AIS which uses E-RNS for better and efficient detector selection. E-RNS incorporate self tuning to make the detectors dissimilar and as a result it achieves greater detector selection ratio. Self tuning also helps NIIAD in building correct and appropriate profile of self and non self even when limited information is available. Self tuning makes NIIAD adaptive which reflect in high detection rate with low false positive for new and unseen test set. Furthermore under different conditions and no matter what would be the training and testing sample NIIAD remains stable. The experimental results firmly illustrate that NIIAD adapts well and reconfigures its profile to recognize self and non-self space effectively and efficiently with high detection rate and low false alarm rate for both existing and new unseen anomalies.

6. REFERENCES

[1] B. Mukerjee, L. T. Heberlein and K. N. Levitt, 1994,"Network Intrusion Detection", IEEE Network, Vol. 8, No.3, pp. 26-41.

[2] D. E. Denning, 1987, "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, Vol. 13, No. 2, pp. 222-232.

[3] D. Dasgupta, 1999, "Immunity-based Intrusion Detection System: A General Framework", in Proceedings of 22nd National Information Systems Security Conference, Arlington, Virginia, USA, pp.147- 160.

[4] D. Dasgupta and S.Forrest 1999, "An Anomaly Detection Algorithm Inspired by the Immune System", Chapter 14 in the book entitled Artificial Immune Systems and their Applications, Publisher: Springer-Verlag, pp. 262–277.

[5] F. Esponda, S.Forrest and P.Helman, 2003 "A Formal Framework for Positive and Negative Detection Schemes",IEEE Transactions on System, Man and Cybernetics, Vol. 34, No. 1, pp 357-373.

[6] F.Gonzalez, D. Dasgupta and J. Gomez, 2003 "The Effect of Binary Matching Rules in Negative Selection",Genetic and Evolutionary Computation Conference (GECCO), Chicago, pp. 383-403

[7] F. A.Gonzalez and D.Dasgupta "Anomaly Detection Using Real-Valued Negative Selection", Genetic Programming and Evolvable Machine,Vol.4. No.4, December 2003, pp. 383-403.

[8] KDD Cup DataSet, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[9] K. Jungwon and P. Bentley, 1999, "The Human Immune System and Network Intrusion Detection", EUFIT 99, pp. 1244-1252.

[10] M. Ayara, J.Timmis, R. Lemos, L.N. de Castro and R.Duncan, 2002, "Negative Selection: How to Generate Detectors", 1st International Conference on Artificial Immune System (ICARIS), UK, pp

[11] M. F. Zafar, F.Naheed, Z.Ahmad and M. M.Anwar, "Network Security: A Survey of Modern Approaches", The Nucleus, 45 (1-2), 27 May 2008, pp 11-31.

[12] P.K.Harmer, P.D. Williams, G.H.Gunsch and G.B.Lamont, June 2002, "An artificial immune system architecture for computer security applications", IEEE transactions on evolutionary computation, Vol.6, No.3, pp. 252–280.

[13] P.Saurabh, B.Verma and S.Sharma, 2012, "Biologically Inspired Computer Security System: The Way Ahead", in Recent Trends in Computer Networks and Distributed Systems Security Communications in Computer and Information Science, Vol, 335, Springer, pp. 474-484.

[14] R.E.Overil, 2007, "Computational immunology and anomaly detection", Information Security Technical Report, Science Direct, Vol.12, pp.188-191.

[15] S.Forrest , A.S.Perelson, L.Allen and R.Cherukuri, 1994, "Self-nonself discrimination in a computer", IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos, CA, pp. 202–212.

[16] S.Ramakrishnan and S.Srinivasan, 2009, "Intelligent agent based artificial immune system for computer security—a review", Artificial Intelligence Review, Vol. 32, No. 1-4, pp 13–43.

[17] S.Forrest, S.A. Hofmeyr and A.Somayaji, 1997, "Computer Immunology," in Communications of the ACM, Vol. 40, No.10, pp. 88–96.

[18] S.T.Powers, J. He ," A hybrid artificial immune system and Self Organising Map for network intrusion detection", in Information Sciences, Vol.178, No.15, August 2008, pp. 3024-3042.

[19] U.Aickelin, J.Greensmith and J.Twycross, 2004, "Immune system approaches to Intrusion Detection- A Review". ICARIS, Springer, pp. 316–329.

[20] W.Wang , X.Guan and X.L.Zhang, 2008, "Processing of massive audit data streams for real-time anomaly intrusion detection", Computer Communications, Vol. 31, No.1, 15, pp.58–72.

[21] Lincoln Laboratory, Massachusetts Institute of Technology, 1999 DARPA, Intrusion detection evaluation data set, Available at: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html

[22] R.Lippmann, J.W. Haines, D.J. Fried , J.Korba, "The 1999 DARPA off-line intrusion detection evaluation", in Computer Networks, Vol. 34, No. 4, October 2000, pp.579-595.

[23] S.W.Lin, K.C.Ying, C.Y.Lee and Z.J.Lee, 2012, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection",in Applied Soft Computing, Vol.12, No.10, pp.3285-3290.