Ensemble Voting based Intrusion Detection Technique using Negative Selection Algorithm

Kuldeep Singh
Department of Computer Science and Engineering,
Punjabi University, Patiala
sidhu.kuldeep89@gmail.com

Lakhwinder Kaur
Department of Computer Science and Engineering,
Punjabi University, Patiala
mahal2k8@gmail.com

Raman Maini
Department of Computer Science and Engineering,
Punjabi University, Patiala
research.raman@gmail.com

Abstract: *This paper proposes an Intrusion Detection Technique (IDT) using an Artificial Immune System (AIS) based on Negative Selection Algorithm (NSA) to distinguish the self and non-self (intrusion) in computer networks. The novelties of the work are 1) use of Stacked Autoencoders (SAEs) and random forest for dimensionality reduction of data, 2) use of AIS to exploit its feature like self-learning, distributed, self-adaption, self-regulation with self and non-self-distinguishing capability, 3) implementation of two algorithms i.e., NSA based on Cosine Distance (NSA_CD) and NSA based on Pearson Distance (NSA_PD) to explore their intrusion detection capabilities, and iv) development of a new ensemble voting based Intrusion Detection Technique (IDT-NSAEV) to detect and test the anomalies in the system. The proposed IDT-NSAEV technique combines the power of NSA_CD, NSA_PD and NSA based on Euclidean distance (NSA_ED) algorithms to enhance the detection rate by reducing the false alarm rate. The performance of the proposed technique is tested on standard benchmark NSL-KDD dataset and the results are compared with the state-of-the-art techniques. The results are in the favour of the proposed technique.*

Keywords: *Artificial immune system, security, negative selection algorithm, anomaly detection.*

Received December 27, 2020; accepted February 28, 2022
https://doi.org/10.34028/iajit/20/2/1

1. Introduction

An Intrusion Detection System (IDS) is the method that attempts to discover the abnormal activities to the computer by analysing the various connection's activities to that system. IDS are mainly categories into two types; Host-based and Network-based IDS [14, 16]. In host-based IDS, the files of the operating system are analysed to find malicious activities, whereas in network-based IDS the incoming traffic of the network is analysed to examine the abnormal behaviour. Further, IDS can be classified into two categories that are Signature-based and Anomaly-based [4] IDS. In signature-based IDS the built-in specific pattern of malicious activities is examined to find malicious behaviour, and in Anomaly-based IDS, the system creates the profile of self and non-self-traffic. Any deviation from the self-profile is considered as an anomaly and reported to the system administrator. In this research work, main focus is on anomaly-based network intrusion detection using Negative Selection Algorithm (NSA).

NSA is a type of Artificial Immune System (AIS), first proposed by Forrest *et al*. [8] to discriminate self and non-self in computer. NSA has two phases, as shown in Figures 1, and 2. In the first phase, the detectors are randomly generated and compared with normal traffic of the network termed as self. The detectors that do not match with self are matured as antibodies used in the future to protect the system from non-self. The matched detectors are removed from the system. In the second phase, the system monitors the new incoming traffic and check for the matching. If there is "No" match, the incoming strings are recursively compared with all the mature detectors. The data or connection's vector that is matched with matured antibodies are identified as anomalies in the system.

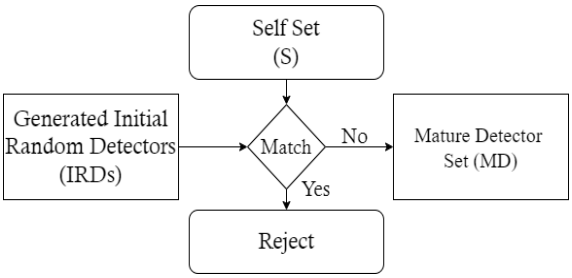

Figure 1. Generation of valid detector set (adopted from [8]).

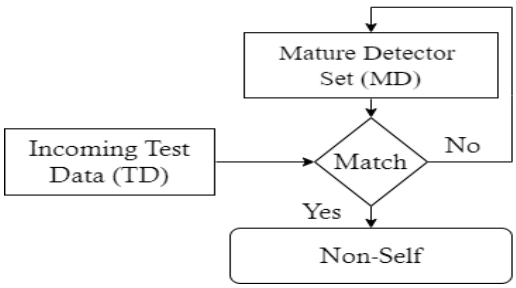

Figure 2. Detection of non-self (adopted from [8]).

This paper is organized as follows. Section 2 describes the related work motivation and contributions of the proposed work. Section 3 describes the proposed work with flow diagrams and algorithms. The Experimental results and analysis are explained in sections 4, and 5 contain the conclusion part.

2. Related Work

The NSA is described by a number of researchers. Its most commonly used representations are binary and real-valued. As any data is ultimately translated to binary bits, therefore, the study focuses on binary representation and AIS coding scheme one of the most widely accepted. Due to string length limitations of binary representation many of the immunity features cannot be expressed. Binary representation is sufficient to depict categorical attributes. Because of these reasons, much of the work in the NSA uses binary representation along with different affinity measures, such as r-contiguous bit matching [8], r-chunk matching [27], Hamming distance [18], and Rogers and Tanimoto (R and T) matching [13]. Forrest *et al*. [8] presented the first binary string theory since it was a finite space that made problem space analysis simple. The NSA splits the 32-bit string into eight substrings, including antigen and antibody. The r-contiguous bit matching technique was used to generate the detectors. To evaluate the performance of their proposed model, they conducted three set of experiments;

1. Using random binary strings.
2. On SPARC intrusions generated by compiling C programs.
3. On COM files infected with computer viruses in Disk Operating System (DOS) environment.

In their experiments the r-contiguous value varied from 1 to 13 and total number of detectors varies from 50 to 100. They demonstrated that their proposed system can detect 50% to 85% of the changes occur in the system. This work was very initial effort to apply the AIS in intrusion detection.

The most works were limited to the binary representation of data and detectors. Subsequently, numerous attempts have been made using different methods to build an effective detector generation algorithm. However, citing the weakness of the NSA algorithm, Gonzalez *et al*. [10] suggested a Real-Valued Negative Selection (RNS) algorithm. The RNS algorithm represents self, detectors and non-self with real-values to resolve the inadequacies of binary representations. The present work will also use real valued NSA. Detectors in the RNS algorithm were n-dimensional vectors with a radius r in the hypersphere. The Euclidean matching function was used to match the detector with any input pattern. Gonzalez *et al*. [9] introduced a randomised, Real-Value, Negative Selection (RRNS) algorithm. This algorithm calculates the number of detectors needed by using the Monte Carlo method to cover non-self-space. They suggested that the number of holes and unaddressed spaces were effectively reduced by using smaller radius detectors, as it requires fewer computations. Stibor *et al*. [23], compared real-valued positive and negative selection algorithms with two other statistical anomaly detection algorithms Support Vector Machine (SVM) and Parzen-Window. The experiment was conducted on high dimensional Knowledge Discovery in Dataset (KDD) dataset and the investigations revealed that the NSA with variables sized detectors is not competent to real valued positive selection algorithm and statistical anomaly detection techniques on KDD dataset. Balachandran *et al*. [6] proposed a system for the generation of multi-form detectors in real-valued NSAs. They extended real-valued NSA by using multi shaped detectors (sphere, rectangle or ellipse) to cover two-dimensional non-self-spaces. Subsequently, Ji and Dasgupta [11, 12] suggested a new real-valued NSA that would produce variable size detectors. Detectors were represented as circles in two-dimensional spaces, and the radii of these circles were variable. On the other hand, Ji and Dasgupta [11] expanded the RNS algorithm with the variable detector radius. This work successfully demonstrated an increase in detection accuracy and protected non-self-space with fewer detectors. They conclude that smaller radius detectors decreased the number of holes and unaddressed spaces.

Yang *et al*. [28] proposed Antigen Space Density-based Real-value NSA (ASD-RNSA) algorithm. The experiment was carried out on Network Security Laboratory-Knowledge Discovery in Databases (NSL-KDD) dataset by using 13390 total number of the detector and have achieved maximum of 92.89% Detection Rate (DR) and 3.47% False Alarm Rate (FAR). They used large number of detectors for detection which slow down the matching procedure's speed. Aziz *et al*. [2] proposed anomaly detection algorithm using Genetic Algorithm (GA) with deterministic crowding Niching technique for detector generation. Euclidian distance is used as a similarity measure in NSA, and the results are tested on NSL-KDD dataset with a maximum of 81.70% DR. Belhadj-Aissa and Guerroumi [7] proposed Network Anomaly Detection Based on Negative Selection process (NADNS). The authors have used the NSL-KDD and kyoto2006+dataset to test their proposed technique. Information gain and correlation attribute evaluation algorithms used for feature selection and achieved the maximum DR of 96% with 18% FAR. Aziz *et al*. [3] compares the Euclidean Distance (ED) and Minkowski Distance (MD) for the artificial immune system-based intrusion detection system. The results are tested on NSL-KDD dataset and showed that the MD has better DR, that is 81.74% as compared to ED, which is

77.44%. They showed the intrusion detection capabilities of MD which can be further enhanced.

The overall discussion and available literature on the NSA indicate that it is capable of reacting to anomaly detection problems. So, in this work NSA based intrusion detection technique has been developed.

- *Research Gaps*:

a) In the literature, most of the researchers have worked on dimensionality reduction either by using feature selection [5, 20] or feature extraction [5, 28] in NSA so, there is room for improvement by exploiting the benefits of both.
b) The literature shows that the concept of deep features was not explored in this domain earlier which can help to speed up the processing and to increase the detection rate [20, 24].
c) As literature shows that most of the work of RNSA used ED [2, 3] with limited work on MD [3] as similarity measures. According to the best of author's knowledge, the similarity measures Pearson distance and Cosine distance are not explored earlier with NSA.

- *This Paper Offers the Following Novel Contributions*:

a) In order to resolve this dimensionality challenge, this work utilizes the hybrid dimensionality reduction technique by combining Stacked Autoencoders (SAEs) for feature extraction and random forest for important feature selection.
b) Implementation of two algorithms i.e., NSA based on Cosine Distance (NSA-CD) and NSA based on Pearson Distance (NSA-PD) to explore their intrusion detection capabilities.
c) Development of a new ensemble voting based Intrusion Detection Technique (IDT-NSAEV) to detect and test the anomalies in the system.
d) The proposed technique improves the attack detection rate and also lower the false alarm rate.

3. Proposed Work

The algorithm works in four steps:

1. Pre-processing and dimensionality reduction.
2. Detector selection.
3. Non-self-detection by individual NSA based upon different similarity measures.
4. Ensemble voting algorithm for accurate non-self-detection.

3.1. Pre-Processing and Dimensionality Reduction

The pre-processing transforms the training as well as test dataset into significant form for efficient processing. Normalization process normalizes pre-processed data in the range of 0 to 1. Dimensionality reduction aids in selecting better-qualified detectors by reducing the search space for the detector. NSL-KDD is most popular, universally acceptable, and recognized dataset [15, 25, 26]. Therefore, in this research work for experimentation, NSL-KDD dataset has been used. This dataset has 1,48,517 records and each record represents a Transmission Control Protocol/Internet Protocol (TCP/IP) link that consists of 41 features plus a "normal" or "attack" mark. This huge number of dimensions makes it very difficult and time-consuming for computation. In order to resolve this dimensionality challenge, this work implements the hybrid dimensionality reduction technique by using Column Standardized Normalization followed by Stacked autoencoders (SAEs) [23] and random forest. Column Standardized Normalization is used to normalize the main network components in the range [0-1]. As shown in Figure 3, hybrid dimensionality reduction algorithm works in two phases. In first phase, the deep features are extracted by SAEs. To reduce the features further, random forest feature selection method has been applied which results in most critical features.

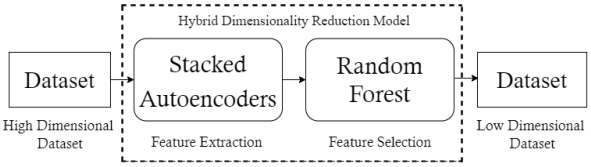

Figure 3. Flow diagram of hybrid dimensionality reduction technique.

3.2. Detector Selection

In this step, the mature detectors are selected based on the three algorithms namely NSA_ED, NSA_CD and NSA_PD. As shown in Algorithm (1) and Figure 4, the Initial Random Detectors (IRD) are matured using three algorithms separately. IRD set containing detectors (d1, d2, ……dn) are n randomly created vectors. Each IRD is matched against the self-set of training data instances by forming a similarity measure matrix. From the similarity measure matrix, for any particular IRD, the closely related affinity value is selected among all the data instances. This indicates that these detectors are how closely related to any data instance. From this closely related list, the detector that has the highest affinity value is selected as a mature detector. All other detectors are dropped out because these detectors are closely related to self-instance. This process is repeated until the desired number of mature detectors are selected from IRD.

Algorithm 1: Detector Selection Algorithm for NSA_ED, NSA_CD and NSA_PD

Step: 1 Start
Step: 2 Generate $IRD_{i=1:n}$, *where* $IRD_i \in R$; $0.0 < IRD_{i,j} < 1.0$
Step: 3 Match all the instances of IRD with TS
Step: 4 Find similarity matric $SM_n x_m$ (* *NSA based on three*

similarity measures) between $IRD_{i=1:n}$ and $TS_{i=1:m}$
Step: 5 Find the minimum matching affinity value corresponds to each detector against all TS instances (Obtained total n values $SM_{i=1:n}$).
Step: 6 Select the maximum value SM_j among $\{SM_{i=1:n}\}$
Step: 7 Corresponding to value SM_j , dx_j is added to the mature detector set list.
Step: 8 Repeat until D_N achieved
Output: Mature detector set MD
** NSA_ED, NSA_CD and NSA_PD*

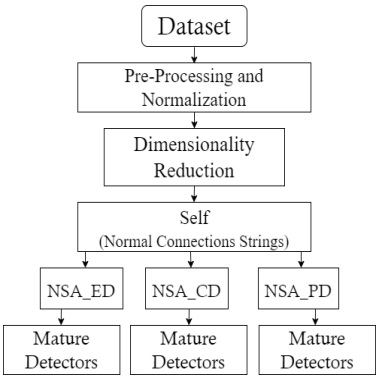

Figure 4. Flow chart of mature detectors selection algorithm.

Although there is a chance that the selected detector is not so mature for every iteration, this problem is solved by self-tuning the mature detectors. Self-tuning of the detector is done based on the ranking value. The detectors that are highly apart from all the instances of training data are marked as highly ranked. Based on this, the highly ranked detectors are selected, and the low ranked detectors are deleted from the list. No doubt this process consumes more time and also the detector rejection rate is also high, but this process increases the power of mature detectors which helps to increase the detection rate.

3.3. Intrusion (Non-Self) Detection

In the third step, mature detectors are used to detect the anomalous (non-self) instance in the data set. As shown in Algorithm (2) and Figure 5, the mature detectors are matched with all test data instance by forming a similarity measure matrix using three similarity measures ED, CD and PD separately. From the similarity matrix, for any particular data instance, the affinity of the all other detectors are calculated from one particular closely related detector. This indicates how far the other detectors are from that particular detector which is matched with that particular test instance. It indicates that this data point may be anomalous, but the final decision is not made based on this single matched detector. All the other affinity values are compared with the binding threshold value. Binding threshold is the affinity value between test data instance and the mature detector. If the compared value of affinity is less than the binding threshold value, then raise the temporary alert alarm. Count all the temporary alert alarm for that particular data instance and compare with the matching threshold. Matching threshold indicates the total number of detectors matched with particular test instance. If the number of alert alarms is more than the matching threshold, then raise the final alarm for non-self; otherwise, data instance is self. This procedure is repeated for all the instances in the test data set. The decisions of NSA with different measures are calculated individually, as shown in Figure 6.

Algorithm 2: Testing phase based on NSA_ED, NSA_CD and NSA_PD

Input: TD, MD, B_T, M_T, where TD=test set ($t_1, t_2, \ldots\ldots t_m$); dx_i=detector; IRD=set of initial random detectors; MD=mature detector set ($d_1, d_2, \ldots\ldots d_n$); SMT_nx_m=similarity matrix having n detectors and m data points; B_T = binding threshold; M_T= Matching threshold; TAA=Temporary alert alarm;
Step: 1 Start
Step: 2 For all instances of $TD_{i=1:m}$
Step: 3 Match all the instance of MD with TD by using similarity measures
Step: 4 Calculate the SMT_nx_m between MD and TD
Step: 5 Calculate how far the other detectors are as compare to one closely related detector to one data instance t_i.
Step: 6 For data instance t_i, if $SMT_{i,j}$<B_T, then increment TAA
Step: 7 Repeat the step 6 for all detectors
Step: 8 If TAA>M_T, then raise the alarm for non self Otherwise, data instance is self
Step: 9 Repeat the step 5 to 8 for all data instances in TD
Output: Data instance having intrusion

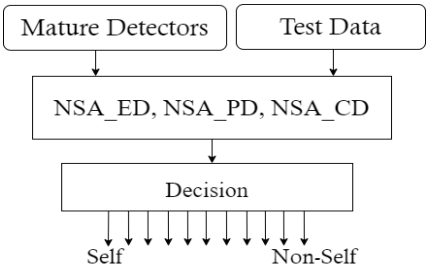

Figure 5. Flow chart of testing of NSA_ED, NSA_CD and NSA_PD algorithms.

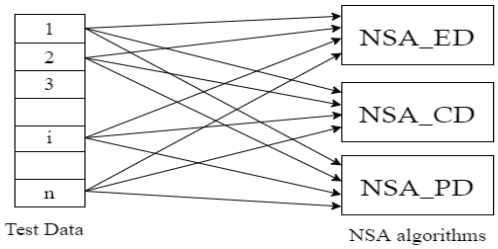

Figure 6. Testing of NSA algorithms with same test instances of NSL-KDD dataset.

3.4. Ensemble Voting

The final testing is carried out in this step of the proposed technique, as shown in Algorithm (3) and Figure 7. The decision of NSA based on different measures has been passed to the ensemble voting algorithm to make the final decision about any test instance. Based on the majority votes, the final decision is made whether the tested data instance is normal or anomalous. The proposed technique

increases the learning rate by rectifying the false decisions made by NSA_ED, NSA_CD and NSA_PD, when runs independently. The proposed NSA_EV improves the performance in term of DR and FAR, by combining the prediction power of the different NSA algorithms.

4. Experimental Results and Analysis

In this paper, all the experiments are carried out on the NSL-KDD dataset on system having Nvidia Graphic Processing Unit version GeForce GTX 1080 with 2560 compute Unified Device Architecture (CUDA) cores and a graphics clocks of 1607 MHz. Python Anaconda tool is used to process the experimental analysis part of the work. NSL-KDD dataset has been commonly used as a reference dataset for identification of anomalies in computer security problems [17]. For experimentation, the test set used in this work consists of 5000 randomly selected undetected data, which includes both self and non-self-data. All the results are computed using the average of 40 runs in the same configuration. The following performance metrics have been used for performance evaluation.

Algorithm 3: Ensemble Voting Algorithm for intrusion detection

Input: A_L, PL_ED, PL_PD, PL_CD; A_L=Actual labels set; PL_ED=predicted labels set of NSA_ED, PL_PD=predicted labels set of NSA_PD; PL_CD=predicted labels set of NSA_CD
Step: 1 Start
Start: 2 Generate voting vector V(i) based on the votes from {PL_ED(i), PL_PD(i), PL_CD(i)}
Start: 3 If V(i)>= two for non_self votes, then raise the alarm as non self
else
data instance is self
Start: 5 Repeat the step 2 and 3 for all A_L
Start: 6 Compare the voting set V with A_L and find the DR and FAR
Output: Data instance having intrusion

4.1. Performance Metrics

DR, FAR [21] and F1-Score are three metrics used to test the efficacy of the proposed technique. DR identifies the rightly classified anomaly by the system, FAR identifies the self is identified as non-self and F1-score measure the predictive power of any classification model. High DR and low FAR are the pre-requirement for any good anomaly detection technique.

1. Detection rate (DR): $\frac{TP}{TP+FN}$* 100, DR is defined as the total number of detected non-self when they are actually non-self.
2. False Alarm Rate (FAR): $\frac{FP}{FP+TN} * 100$, FAR is defined as the total number of detected non-self when they are actually self.
3. F1-Score: $2\ \frac{Precision\ .Recall}{Precision+Recall}$, it is a measure of the harmonic mean of precision and recall which represents the predictive power of any classification model.

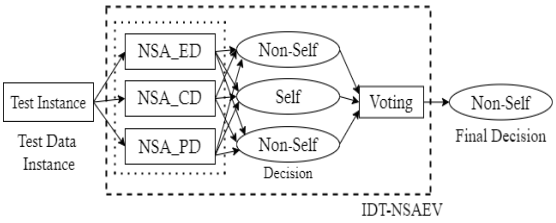

Figure 7. Flow diagram of ensemble voting algorithm.

4.2. Dimensionality Reduction

This work has used the column standardization technique [22] for normalization of dataset, followed by proposed hybrid dimensionality reduction technique i.e., combination of stacked autoencoders [22] feature extractor method and random forest feature selection method. Stacked autoencoders [22] reduces from 41 features in NSL-KDD to 30 features. Next, the application of random forest feature selection method reduces the features further from 30 to 12. This reduction in dimensionality of dataset will lead to reduction in computational complexity for further processing.

4.3. Selection of Stable Threshold

Table 1 shows the variations in DR and FAR by changing with the Binding threshold values. As shown in table, the NSA_ED has 92.68% DR and 28.79% FAR at affinity value 0.35. The highest value of DR is 94.8% with minimum FAR (18.97%) at affinity value 0.4. Beyond this, with the increase of Binding threshold value, the DR decreases and FAR also increases. Similarly, for NSA_PD the average value of Binding threshold is 0.45 at which it gives highest DR (95.27%) with 23.56% FAR, and for NSA_CD the affinity value 0.55 gives highest DR (94.4%) with 28.07 FAR. From the results, binding threshold 0.40 for NSA_ED, 0.55 for NSA_CD and 0.45 for NSA_PD is chosen for further performance evaluations.

Table 1. Optimum threshold value selection for NSA_ED, NSA_CD and NSA_PD.

Binding Threshold	NSA_ED		NSA_CD		NSA_PD	
	DR	FAR	DR	FAR	DR	FAR
0.35	92.68	28.79	80.23	43.23	93.22	54.3
0.40	**94.8**	**18.97**	87.44	26.96	89.36	24.64
0.45	90.19	24.94	90.71	26.44	**95.27**	**23.56**
0.50	86.86	23.19	91.09	27.19	88.63	23.56
0.55	80.55	30.26	**94.4**	**28.07**	83.91	24.71
0.60	73.29	40.67	94.78	59.4	47.36	7.16

4.4. Selection of Number of Detectors

Table 2 illustrates the results obtained by NSA_PD, NSA_CD and NSA_ED, by changing the number of detectors. The values in the table demonstrated that as the number of detectors is 20 in NSA_ED, the obtained DR is 94.8% and FAR is 18.97%, which is

comparatively better performance as we increase the number of detectors. As the number of detectors increases the DR decreases and FAR rate increases. Similarly, NSA_CD gives the stable performance at 20 detectors, and NSA_PD has highest DR and lowest FAR at 25 number of detectors as shown in table. Beyond this, As the number of detectors is increased, the performance goes down. From the results, the number of detectors 25 for NSA_PD, and 20 for NSA_ED as well as for NSA_CD has been chosen for further performance evaluations.

Table 2. Selection of number of Detectors for NSA_PD, NSA_CD and NSA_ED.

Detectors	NSA_ED		NSA_CD		NSA_PD	
	DR	FAR	DR	FAR	DR	FAR
10	91.37	22.16	91.34	32.30	92.30	26.34
15	94.71	25.62	92.77	31.31	94.35	25.77
20	**94.8**	**18.97**	**94.41**	**28.07**	94.07	28.97
25	94.27	29.52	92.5	30.15	**95.27**	**23.56**
30	90.55	31.76	91.59	31.16	93.77	29.24
35	87.41	27.1	91.20	30.24	91.82	27.76
50	87.36	28.65	90.08	28.48	90.53	28.21

4.5. Performance of Proposed Technique (IDT-Nsaev)

Table 3 illustrates the performance of proposed technique in terms of DR, FAR and f1 score. Since, the proposed model combines the predictive power of three algorithms namely; NSA_ED, NSA_CD and NSA_PD. It increases the DR to 97.52% which is highest among the state of the arts techniques. Also, it reduces the FAR to 11.67% which is lower than NSA based algorithms compared in the table. Hence, it is experimentally evident that the proposed IDT-NSAEV technique enhances the prediction power by increasing the DR.

Table 3. Results of proposed ensemble voting algorithm in comparison of other three algorithms.

Algorithm	DR	FAR	f1 score
Proposed IDT-NSAEV	**97.52%**	**11.67%**	**0.864865**
NSA_PD	95.27%	23.56%	0.859544
NSA_ED	94.08%	18.97%	0.841142
NSA_CD	94.40%	28.07%	0.8202

Table 4. Comparison of proposed Intrusion detection technique with other related techniques.

Technique	SM	Dataset	DR	FAR
Proposed IDT-NSAEV	ED, PD and CD	NSL-KDD	**97.52%**	**11.67%**
NSA-ED	ED	NSL-KDD	94.08%	18.97%
NSA-PD	PD	NSL-KDD	95.27%	23.56%
NSA-CD	CD	NSL-KDD	94.40%	28.07%
NSA with GA and DCN [2]	ED	----	81.70%	----
NADNS [7]	----	NSL-KDD kyoto2006+	96%	18%
AIS inspired IDS based on GA [3]	ED, MD	NSL-KDD	81.74 % -ED 77.44%-MD	----
RS based AIRS [19]	----	NSL-KDD	39.89%	----
MA-AIS [1]	----	NSL-KDD	89.78%	12.67%
MAIS-IDS [20]	----	NSL-KDD	90.54%	29.72%

4.6. Comparison with the Related Work

To demonstrate the efficacy of the proposed technique, the results are compared with the other state-of-the-art intrusion detection techniques in terms of DR and FAR. Table 4 shows the comparison of the proposed technique with existing NSA based intrusion detection techniques on NSL-KDD dataset. The table shows that the proposed method has achieved DR on average 97.52% which is 1.52% higher than the higher than the state of the arts techniques. The proposed technique also lowers the FAR to 11.67% which is lesser as compared to the other techniques.

5. Conclusions

This work proposed an ensemble voting based intrusion detection technique in computer networks using NSA abbreviated as IDT-NSAEV. First, the hybrid dimensionality reduction approach based on SAEs followed by random forest has been implemented, in order to reduce the dimensions of the data. Second, NSA based on CD and PD has been developed to explore their prediction power for intrusion detection. Results are taken on NSL-KDD dataset and compared with traditional method NSA based on ED. From the results, it has been analysed that although the average performance of these algorithms is comparable in terms of DR but individually, they are not showing stable behaviour. In order to address this problem a new IDT-NSAEV has been proposed by combining the predictive power of NSA_ED, NSA_CD and NSA_PD algorithms. The proposed technique achieved an average DR of 97.52% which is higher than 1.52% as compared to state of the arts techniques using NSA. The Proposed technique reduces the FAR. For the future work, the possibilities can be explored by combining the other similarity measures like Manhattan distance, Minkowski Distance etc. with the proposed technique.

- *Funding*: This work is supported by Visvesvaraya PhD scheme of Ministry of Electronics and Information Technology (MeitY), Government of India under the Award number 11337.

References

[1] Aziz A., Hanafi S., and Hassanien A., "Multi-Agent Artificial Immune System for Network Intrusion Detection and Classification," *in Proceedings of International Joint Conference SOCO'14-CISIS'14-ICEUTE'14*, Bilbao, pp. 145-154, 2014.

[2] Aziz A., Salama M., Hassanien A., and Hanafi S., "Detectors Generation Using Genetic Algorithm for A Negative Selection Inspired Anomaly Network Intrusion Detection System," *in Proceedings of Federated Conference on*

Computer Science and Information Systems, Wroclaw, pp. 597-602, 2012.

[3] Aziz A., Salama M., Hassanien A., and Hanafi S., "Artificial Immune System Inspired Intrusion Detection System using Genetic Algorithm," *Informatica*, vol. 36, no. 4, pp. 347-358, 2012.

[4] Aldweesh A., Derhab A., and Emam A., "Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems: A Survey, Taxonomy, and Open Issues," *Knowledge-Based Systems*, vol. 189, pp. 105124, 2020.

[5] Abid A., Khan M., and de Silva C., "Layered and Real-Valued Negative Selection Algorithm for Fault Detection," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2960-2969, 2017.

[6] Balachandran S., Dasgupta D., Nino F., and Garrett D., "A Framework for Evolving Multi-Shaped Detectors in Negative Selection," *in Proceedings of IEEE Symposium on Foundations of Computational Intelligence*, Honolulu, pp. 401-408, 2007.

[7] Belhadj-Aissa N. and Guerroumi M., "A New Classification Process for Network Anomaly Detection Based on Negative Selection Mechanism," *in Proceedings of International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Zhangjiajie, pp. 238-248, 2016.

[8] Forrest S., Perelson A., Allen L., and Cherukuri R., "Self-Nonself Discrimination in A Computer," *in Proceedings of IEEE Computer Society Symposium on Research In Security and Privacy*, Oakland, pp. 202-212, 1994.

[9] González F., Dasgupta D., and Gómez J., "The Effect of Binary Matching Rules in Negative Selection," *in Proceedings of Genetic and Evolutionary Computation Conference*, Chicago, pp. 195-206, 2003.

[10] Gonzalez F., Dasgupta D., and Niño L., "A Randomized Real-Valued Negative Selection Algorithm," *in Proceedings of International Conference on Artificial Immune Systems*, pp. 261-272, 2003.

[11] Ji Z. and Dasgupta D., "Real-Valued Negative Selection Algorithm with Variable-Sized Detectors," *in Proceedings of Genetic and Evolutionary Computation Conference*, USA, pp. 287-298, 2004.

[12] Ji Z. and Dasgupta D., "Applicability Issues of The Real-Valued Negative Selection Algorithms," *in Proceedings of the 8th Annual Conference on Genetic and Evolutionary Computation*, Seattle, pp. 111-118, 2006.

[13] Ji Z. and Dasgupta D., "Revisiting Negative Selection Algorithms," *Evolutionary Computation*, vol. 15, no. 2, pp. 223-251, 2007.

[14] Liu M., Xue Z., Xu X., Zhong C., and Chen J., "Host-Based Intrusion Detection System with System Calls: Review and Future Trends," *ACM Computing Surveys (CSUR)*, vol. 51, no. 5, pp. 1-36, 2018.

[15] McHugh J., "Testing Intrusion Detection Systems: A Critique of The 1998 and 1999 Darpa Intrusion Detection System Evaluations as Performed by Lincoln Laboratory," *ACM Transactions on Information and System Security*, vol. 3, no. 4, pp. 262-294, 2000.

[16] Meftah S., Rachidi T., and Assem N., "Network Based Intrusion Detection using the UNSW-NB15 Dataset," *International Journal of Computing and Digital Systems*, vol. 8, no. 5, pp. 478-487, 2019.

[17] Powers S. and He J., "A Hybrid Artificial Immune System and Self-Organising Map for Network Intrusion Detection," *Information Sciences*, vol. 178, no. 15, pp. 3024-3042, 2008.

[18] Poggiolini M. and Engelbrecht A., "Application of the Feature-Detection Rule to the Negative Selection Algorithm," *Expert Systems with Applications*, vol. 40, no. 8, pp. 3001-3014, 2013.

[19] Sabri F., Norwawi., and Seman K., "Hybrid of Rough Set Theory and Artificial Immune Recognition System as A Solution to Decrease False Alarm Rate in Intrusion Detection System," *in Proceedings of 7th International Conference on Information Assurance and Security*, Melacca, pp. 134-138, 2011.

[20] Seresht N. and Azmi R., "MAIS-IDS: A Distributed Intrusion Detection System Using Multi-Agent AIS Approach," *Engineering Applications of Artificial Intelligence*, vol. 35, pp. 86-298, 2014.

[21] Silva G., Caminhas W., and Palhares R., "Artificial Immune Systems Applied to Fault Detection and Isolation: A Brief Review of Immune Response-Based Approaches and A Case Study," *Applied Soft Computing*, vol. 57, pp. 118-131, 2017.

[22] Singh K., Kaur l., and Maini R., "Efficient Intrusion Detection Technique Using Stacked Autoencoder," *Advances in Mathematics: Scientific Journal*, vol. 9, no. 6, pp. 3839-3848, 2020

[23] Stibor T., Timmis J., and Eckert C., "A Comparative Study of Real-Valued Negative Selection to Statistical Anomaly Detection Techniques," *in Proceedings of International Conference on Artificial Immune Systems*, Banff, pp. 262-275, 2005.

[24] Saurabh P. and Verma B., "An Efficient Proactive Artificial Immune System Based Anomaly Detection and Prevention System," *Expert Systems with Applications*, vol. 60, pp. 311-320, 2016.

[25] Tavallaee M., Bagheri E., Lu W., and Ghorbani A., "A Detailed Analysis of The KDD CUP 99

Data Set," *in Proceedings of Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, pp. 1-6, 2009.

[26] Tabash M., Abd Allah M., and Tawfik B., "Intrusion Detection Model Using Naive Bayes and Deep Learning Technique," *The International Arab Journal of Information Technology*, vol. 17, no. 2, pp. 215-224, 2020.

[27] Van-Truong N. and Hoai N., "A Novel Negative Selection Algorithm with Optimal Worst-Case Training Time Complexity for R-Chunk Detectors," *Indian Journal of Science and Technology*, vol. 13, no. 10, pp. 1160-1171, 2020.

[28] Yang T., Wen C., and Tao L., "An Antigen Space Density Based Real-Value Negative Selection Algorithm," *Applied Soft Computing*, vol. 61, pp. 860-874, 2017.

Kuldeep Singh was born in Bathinda, Punjab India. He graduated and received his M. Tech. degree in 2015 in the field of Computer Science and Engineering from Punjabi University, Patiala. In 2016, he enrolled himself as doctoral student, PhD, at the Punjabi University, Patiala, Punjab, India. His research interest is focused on Network Security, Intrusion Detection System, MANET, Machine Learning.

Lakhwinder Kaur is a Professor in Computer Engineering at Punjabi University, Patiala, India. She received her PhD from PTU, Jalandhar, India. She has been in teaching since September 1992. Her research interest includes image processing, wireless networks and Network Security. She has published many research papers in International Journals, Conference proceedings as well as books.

Raman Maini received B.Tech. (Computer Science and Engineering) from Beant College of Engineering, Gurdaspur, Punjab, India in 1999 and M. Tech. (Computer Science and Engineering) from PAU, Ludhiana, India, in 2002. He got Merit certificate in his M. Tech. thesis at PAU. He is currently working as a Professor in Computer Engineering at University College of Engineering, Punjabi University, Patiala, India. He is a life member of ISTE (Indian Society of Technical Education), India and IETE (Institution of Electronics and Telecommunication Engineers), India. His current area of research is Network Security, Intrusion Detection System, Computer Vision (Specialty Noise Reduction in Medical Images, Edge Detection and Image Enhancement), development of soft computing-based algorithms.