PERFORMANCE EVALUATION OF ARTIFICIAL IMMUNE SYSTEM ALGORITHMS FOR INTRUSION DETECTION

[*1] Akinwande, O.T and [2] Abdullahi, M.B
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
*Email of Corresponding Author: oladayoakinwande@yahoo.com

ABSTRACT

The need for real network traffic and large-scale realistic intrusion detection datasets in order to improve performances of IDS systems has make the use of Artificial immune system techniques to be on the rise. A dataset that contains benign and common attack network flows that mimics the real time can only help to train and test an intrusion detection system. In this paper, anomaly-based intrusion detection models are built using AIS algorithms namely AIRS1, Immunos, ClonalG and Dendritic Cell Algorithms. These algorithms were tested with NSL-KDD and CICIDS 2017 datasets, which have common updated set of malicious attacks such as DDoS, XSS, SQL Injection, Infiltration, Bruteforce, Portscan and Botnet. Our experiments show that AIS algorithms generally performs better both in accuracy and precison in detecting new attacks than other classifiers .

Keywords: Artificial Immune System, Anomaly, Feature Selection, Intrusion Detection, Network Security, Classification Algorithms

1.0 INTRODUCTION

The advances in computer networks and related applications not only have made it easier to access information anywhere anytime but have also made potential threats to the global information network infrastructure to be on the rise. This security challenge has necessitated for a special attack and misuse detection system, which intrusion detection system (IDS) is a good solution. This paper is an extension of the work presented in [1]. Intrusion detection system, therefore, provide a well-established mechanism to protect infrastructure of network system by gathering and analyzing information from various areas within a host or a network to identify possible security breaches [2]. Intrusion detection systems are built on the assumption that abnormal activities (anomaly) are obvious and noticeable.

A variety techniques have been applied to anomaly detection and building of intrusion detection systems, which include neural networks [2], Statistical learning algorithms [3] and Artificial immune systems algorithms [4]. Artificial Immune System (AIS) is a relatively new research area, which has been studied and applied to intrusion detection system. AIS is a class of algorithms that is inspired by the principles and functioning of the biological immune system. These algorithms [5] exploit the characteristics of the biological immune system in terms of learning and memory as means of solving complex problems.

Different AIS techniques are been used in the development of anomaly intrusion detection system [6]. They could be adaptive, innate and lightweight. Such techniques include negative selection algorithm (NSA), clonal selection algorithm (CLONALG), artificial immune recognition system (AIRS) and dendritic cell algorithm (DCA) [7]. AIS can be considered as a strong candidate for anomaly detection as it discriminate between self and non-self-data. It can be applied for small and medium domains of anomaly detection. It has also been applied to various problem domain such as document classification, fraud detection, network and host-based intrusion [8].

However, the researches that conduct performance comparison among AIS algorithms are limited especially in the use of different IDS datasets with large dimensionality and up-to-date attacks. [9] used DARPA dataset for intrusion detection system evaluation which has the same attack category as KDD Cup 99. Their evaluation confirmed that DOS and R2L attacks are very difficult to observe for an anomaly by an anomaly detector. The reason is that both attacks have a very low variance in the dataset. This drawback will not be able to know whether a design model is capable of detecting such attacks.

[10] aimed at improving the detection accuracy of IDS by using negative selection algorithms and KDD Cup 99 as their test dataset. The IDS makes use of rough set as its optimised feature selection which produced a significant increase in accuracy and true negatives (TN). Both KDD Cup 99 and DARPA 2000 have been widely used by researchers in IDS [11] but may not be representative of the performance with more recent attacks or with other attacks against different types of machine, routers and firewalls [9].

[12], listed evaluation criteria necessary for a dataset and these are discussed in [13]. They are; complete network configuration, complete traffic, labelled dataset, complete interaction, complete capture, common available protocols, attack diversity, heterogeneity, feature set and metadata. Although, NSL-KDD didn’t meet all this criteria but being one of the widely used IDS dataset as at now which has also improved over its original version, we consider its large dimensionality and its acceptability for baseline comparison with CICIDS 2017 datasets.

The aim of this paper is to evaluate the performance of AIRS1, ClonalG , Immunos1 and dendritic cell algorithms on_Network Socket Layer-Knowledge Data Discovery (NSL-KDD) dataset and Canadian Institute of Cybersecurity Intrusion Detection System (CICIDS 2017) dataset in terms of classification accuracy for anomaly-based intrusion detection system. The reasons for preferring these algorithms in this work are;   AIRS1, ClonalG , and Immunos1 algorithms are designed as supervised algorithms for classification problem domain [14] except for dendritic cells algorithms which is designed as unsupervised algorithm and the capability of detection has been imitated in artificial immune systems for intrusion detection, which is the basic principle of AIRS1, Immunos1 and ClonalG [15][7]. This paper is organized as follows. The section 2 discussed some research work in intrusion detection system. In section 3, the description of the experiments and the methods are explained. Section 4 presented the results obtained. Conclusion and future work is given in section 5.

2.0 LITERATURE REVIEW

A. Artificial Immune Systems Algorithms

IMMUNOS1 algorithm is an artificial immune system based algorithm which assumes no data reduction, thus the clone population prepared is maintained and is used to classify unknown data instances. The artificial immune network algorithms includes the base version and the extension for optimization problems called the optimization artificial immune network algorithm [9].

The clonal selection algorithm (CLONALG) is actuated from the clonal selection theory. Clonal selection theory is a scientific theory in immunology that explains the functions of cells (lymphocytes) of the immune system in response to specific antigens attacking the body. The theory states that the antibodies select the antigens based on the selection which further produces its clones for antibody production. The mutation occurs to allow the variations in cloned cells [9][7]. The selection of antibodies for cloning is inspired by Darwinian natural selection theory of evolution. Clonal Selection algorithm is a self-organized. It is applied to optimization, classification and pattern recognition problem. The stepwise for this algorithm is described in figure 1.

1) Initialisation:

 An antibody pool of fixed size ***P*** is prepared.

 The pool of size ***P*** is divided into two components i.e.

memory pool ***m*** and remainder pool ***r***.

 Memory pool m is used to act as a representative of the algorithms whereas the remainder pool ***r*** is used for introducing additional diversity into the system.

2) Main loop:

 The algorithm is then advanced by running a number of iterations by exposing the system to all known antigens. There are several number of iterations ***G*** where the number of iterations is user configurable.

 The system is exposed to all the known antigens.

 One antigen among the pool of antigens is selected randomly.

 The antigen is allowed to act on the system.

 Affinity is measured for each antibody against the selected antigen (Affinity: attraction between an antibody and an antigen).

 n number of antibodies are chosen from the whole antibody pool having the highest affinity against the antigen.

 The selected ***n*** number of antibodies are cloned according to their affinity (somatic hyper mutation).

 Mutation of the cloned antibodies are done so as to yield better affinity against the antigen from testing data.

 The cloned antibodies are then allowed to act on the antigen and affinity is measured for each antibody.

 The cloned antibody or antibodies with the highest affinity is selected as a candidate memory antibodies to form a part of memory pool ***m***.

 Lastly, the ***d*** individuals with the lowest affinity in the remaining pool ***r*** are replaced with new random antibodies.

3) Finish:

 After the training rule is completed, the memory pool m which is the component of antigen pool is considered as the solution of the algorithm[12].

Figure 1 : A. Stepwise Algorithm For CLONALG [7]

In AIRS, clonal expansion and affinity maturation are used to encourage the generation of potential memory cells which are later used for classification. Hypothetically, AIRS has four stages to learning which are initialization, memory cell identification, resource competition and finally; refinement of established memory cells. The original AIRS1 algorithm uses a user defined *mutate rate* parameter to determine the degree to mutate a produced clone, and simply replaced attribute values with randomly generated values within the attributes normalised range. The stepwise details of AIRS1 algorithm is described in Figure 2. AIRS2 introduced the concept of somatic hyper mutation where the amount of mutation a clone receives is proportional to its affinity to the antigen in question [7]. In this study, only the AIRS1 will be used for our experiment.

1) Initialisation:

- Firstly this step of the AIRS algorithm aims at adjusting the data for use in the training process and adjusting the system variables.
- The training data is ordered such that the range of each numeric attribute is the range [0, 1] of each numeric attribute.
- An affinity measure is required for use through the training process.

2) Antigen training:

- This algorithm needs loading before each shot and only one pass over the training data.
- The recognition cells in the memory pool are stimulated by the antigen and each cell is allocated a stimulation value (inverted affinity).
- The memory cell with the greatest stimulation is then selected as the best match memory cell for use in the affinity maturation process.

3) Competition for limited resources:

- After addition of a number of mutated clones from the best matching memory cell to ARB pool, the process of ARB generation and competition starts.
- Competition for limited resources is used to administer the size of the ARB pool and acquire ARBs with high affinity to the antigen being trained on.
- A no. of mutated clones are then created from the selected memory cell and added to the ARB (Artificial Recognition Ball) pool.

4) Memory cell selection:

- When the stop process for the ARB refinement is completed, the ARB with the highest normalized affinity measure is taken to become the memory cell candidate.
- The selected ARB is copied into the memory cell pool if the candidate is greater than that of the original best matching memory cell.
- Before removing the original best matching memory cell it is being checked. This occurs only if the affinity between the candidate memory cell and the best matching cell is below a cut-off.

5) Classification:

- When the training process is finished, the pool of memory recognition cells become the core of the AIRS classifier.
- The data vectors contained within the cells are left as it is for the classification process.
- Classification occurs via k-nearest neighbor approach where the ***k*** best matches to a data instances are located and the class is determined using majority vote.
- In this process, only ARBs of the same class as the antigens are taken.
- The last step looks each ARB in the pool to have mutated clones generated using the same clonal methods

Figure 2: Stepwise algorithm for AIRS1 [21]

Dendritic cell algorithm is a relatively recent approach in machine learning inspired by the function of the immune system using dendritic cells. AIS based solutions for mining network data has received considerably growing attention from researchers to strengthen the resilience of information systems against various types of malicious activities [15]. Based on Danger theory, immune response on natural systems is a result of sensing corruption as well as sensing unknown substances. the properties of DCA such as robustness and self-organization has make it more sophisticated than NSA, clonal which has scaling and high rate of false negatives generation issues. Danger theory has some properties which makes it a suitable model for intrusion detection system. Properties such as dynamical system, evolutionary algorithms, immune memory, natural computation and optimization [16]. Details about this algorithms is given in figure 3.

DC presents incorrect information, it becomes inconsequential provided that the majority of DCs derive the correct context. The sampling of data is combined with context information received during the antigen collection process. Different combinations of input signals result in two different antigen contexts. Semi-mature antigen context implies antigen data was collected under normal conditions, whereas a mature antigen context signifies a potentially anomalous data item. The nature of the response is determined by measuring the number of DCs that are fully mature, represented by a value, MCAV - the mature context antigen value. If the DCA functions as intended, the closer this value is to 1, the greater the probability that the antigen is anomalous. The MCAV value is used to assess the degree of anomaly of a given antigen. By applying thresholds at various levels, analysis can be performed to assess the anomaly detection capabilities of the algorithm.

The DCA has three stages: initialisation, update and aggregation. Initialisation involves setting various parameters and is followed by the update stage. The signals used for our DCA is given in Table 2 for NSL-KDD dataset. Finally, the aggregation stage is initiated, where all collected antigen are subsequently analysed and the MCAV per antigen are derived.

```
Input: Antigen(IP Address) and Signals(Safe, Pamp, Danger)
(SS, PAMP, DS and antigens).
Output: antigen and their context values; (0/1).
Parameters: Migration threshold, anomaly threshold
initialize-DC();
for each cell in DC Population do /*Initialization stage */
(
while CSM Output Signal < migration threshold do /* Data processing stage */
get antigens();
Sore antigen
get-signals();
calculate-interim output signals();
update-cumulative output signals();
)
If Semi-mature output(O2) > mature output (O3)
Cell context is assigned as 0;
Else
Cell context is assigned as 1;
Kill cell;
Replace cell in population;
```

Figure 3: Dendritic Cell Algorithms

B. Related Works

During detection, anything that deviates from the normal profile is classified as anomalous and an alarm is launched. It is on this principle intrusion detection systems are built. There are various approaches for anomaly based IDS. They are statistically based intrusion detection, rule based detection and signature based detection. According to [6], anomaly-based detection discriminate between normal and anomalous data based on the knowledge of the normal data. Normal data is created when the system first generate profiles of normality by either training or statistical analysis. The main problem is defining the boundary between acceptable and anomalous behaviour. The concept of normality is needed in order to provide an appropriate solution in network anomaly detection [16]. Therefore, the anomaly detector approaches must be able to distinguish between the anomaly and normal data.

[17] built predictive models for intrusion detection using machine classification algorithms namely logistic regression, Gaussian Naives Bayes, support vector machine (SVM) and random forest using NSL-KDD dataset. The experimental results show that Random Forest Classifier out performed all other methods in identifying whether the data traffic is a normal or an attack.

[15] have used clonal Selection algorithms as classifier. The result of their experiment was compared with other classifier such as J48, Naïve Bayes, SVM, and MLP based on accuracy using the KDD CUP-99 dataset. Clonal selection algorithm performs better than other classifier.

[18] analysed ClonalG and Immnuos1 on the subset of the NSL-KDD dataset, which contained more of anomalous records, compares to normal records. The ClonalG perform better in detecting anomalous packets over the compared classifiers, which are naïve bayes and immunos1. There is a slight difference in the performance of ClonalG and Immnos1 in their work. ClonalG has 78.66% accuracy while Immunos1 has 77.93% accuracy.

AIS algorithms has also been used on some other benchmark dataset [19][20], which are not intrusion dataset. The same has been compared with non-AIS based data mining algorithm such ZeroR, J48, naïve bayes and the AIS algorithms especially AIRS, which demonstrated a superior performance[22].

[14] described the analysis and comparison of different datasets using different AIS based classification algorithms. They further compare different datasets through the different AIS and non-AIS based algorithms to select the best suitable algorithm for the corresponding dataset. Breast cancer, Ecoli, Hepatitis, Pima Indian and Heartstatlog dataset were used in their study. AIRS1 perform much better than ClonalG and Immnos1 in accuracy, specificity and sensitivity using all the dataset. Based on accuracy, AIRS1 achieved 97.42% in Breast cancer, 82.44% in Ecoli, 81.94% in Hepatitis, 72% in Prima Indian and 76.29% in Heartstatlog.

[4] described an intrusion detection approach modeled on the basis of two bio-inspired concepts namely, negative selection and clonal selection. Their intrusion detection system model incorporates a knowledge base constructed by ClonalG using negative selection and uses ClonalG for recognition of the malicious activities in the system. Their proposed model is hoped to perform efficiently in real-time environments.

[23] Introduced auto-immune DCA and auto immune K-means to improve accuracy, detection rate and decrease false alarm for the DCA. Their results show that their model is effective than previous model but the KDD dataset was use for testing which may not to suffice for other standard intrusion dataset. [24]presents a system for detecting DOS attack in a network using the dendritic cell algorithms. Their systems classifies incoming network traffic into normal or DOS attack using NSL-KDD dataset but their system

3.0 METHODOLOGY

Our work is to design an anomaly-based intrusion detection system with different AIS Classifiers. The process used is described as follow.

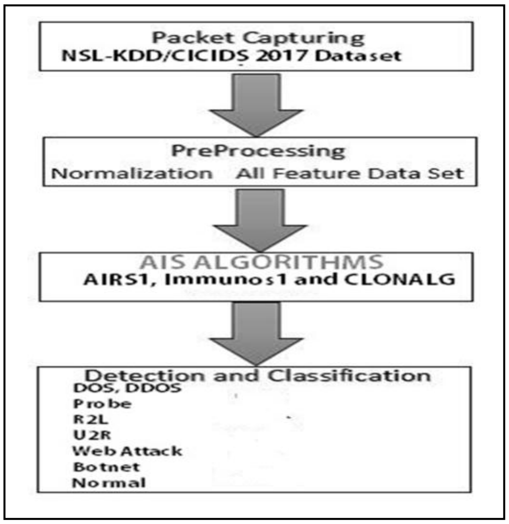


Figure 4: Research Process Framework

A. Dataset Description

In our work of anomaly and intrusion detection over the network, data are gathered in form of packet capture (pcap). For this work, we used NSL-KDD and CICIDS dataset. The extracted packet capture (pcap) are now converted to common separated value (CSVs) files which are imported into the Explorer view of the WEKA tool and MATLAB for further processing. Weka is a collection of machine learning algorithms for data mining tasks. The algorithms can either be applied directly to a dataset or called from your own Java code.

NSL-KDD data set is a publically available data set which is offline network data based on KDD 99 data set [22]. CICIDS dataset can also be accessed from the UNBCSX archive based on request [25].

NSL-KDD data set is a new version of the KDD ’99 data set. It is a network traffic data set. NSL-KDD train and test sets have a reasonable number of records which makes it affordable to run experiments on the complete set without the need to randomly select a small portion. This advantage has make evaluation results of different research work to be consistent and comparable. NSL-KDD data set consists of 41 features. Not all these 41 features are equally important. Some of these features may decrease the performance and accuracy of the Intrusion Detection System. The NSL-KDD has some advantages over the original KDD data set:

i. Redundant records are not present in the train set which will make the classification problem not to be biased if more frequent records are present.

ii. It gives better detection rates on the frequent records as there is no duplicate records in the proposed test sets.

The NSL-KDD also has its own deficiencies. The huge redundant records in the dataset in the datasets makes the learning algorithms to be biased towards the frequent records and this prevent the dataset to learn from unfrequently records, which are usually more harmful to network such as User2Root. Table 1 presented the attacks, which NSL-KDD simulated.

The CICIDS 2017 dataset consists of labelled network flows, including full packet payloads in packet capture (pcap) format, the corresponding profiles and the labelled flows in common separated values (CSVs) format[25]. In computer network administration, the packet capture consists of an application programming interface (API) for capturing network traffic. CICIDS 2017 dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). The datasets consist of 85 attributes and a Class for each of the attack categories and instances for each of the attack categories are much more than the NSL-KDD. The CICIDS dataset has attack diversity by including most common attacks such as web based, brute force, Dos, DDos, infiltration, Heartbleed, Bot, and scan [26]. It is because of these large log files of packets that have been extracted into CSV formats that feature selection techniques used in this study will be discussed in the data preprocessing section.

Table 1. **Attack_Types for NSL-KDD**

DOS	**Probe**	**R2L**	**U2R**
back	ipsep	ftp-attack	bufferoverflow
land	nmap	Guess_password	loadmodule
neptune	portseep	lmp	perl
pod	satan	multilp	rootkit
smurf		phf	
teardrop		spy	
		warezclient	
		warezmaster	

B. **Data Preprocessing**

Pre-processing is carried out in order to convert raw network traffic profiles into quality traffic profiles and used in future as data source for developing the IDS. The quality traffic profiles consist of normal and attack profiles are given as input to the intelligent misuse intrusion detection subsystem to detect known attacks. NSL-KDD and CICIDS 2017 dataset has been considered as the data source for evaluating the performance of our IDS.

Redundancy Removal

Both dataset are developed in a simulated network environment .The collected traffic features are found to exhibit redundancy in both normal and attack profiles [13]. The detection model, if developed with these features as such is likely to be biased towards redundant instances. Hence, the instances need to be processed for redundancy removal which helps in reducing the number of duplicated instances. In this work, removal of redundant instances is carried out only on CICIDS 2017 dataset using the (RemoveDuplicates) feature of the Weka preprocessing tool. The NSL-KDD don’t have a redundant record as this is one of the improvement it has over the KDD CUP-99 dataset. In the case of CICCIDS, further processing was also carried which is of the limitation of the work presented in [1] and this limit the work in the number of attack that was simulated. The NAN value in the dataset were replaced with 0 while the infinite value were replaced with 1.

Normalization using the Min-Max Scaling

A suitable normalization technique is necessary to reduce the domination of features with higher values over features with lesser values so that the detection model would not be biased towards features having higher values [29] In this work, normalization is carried out to transform values of all features into a common specific range by using the Min-Max scaling technique. The formulae for the normalization is giving below:

$$zi = \frac{xi - \min(x)}{\max(x) - \min(x)}$$

C. Feature Selection

Part of this study was to compare the performance of classifiers based on the features selected. By omitting attributes that do not contribute to the efficacy as well as efficiency of the algorithm, there was reduction in the dimensionality of our data set and this improved the processing performance. A more efficient search strategies and evaluation criteria are needed for feature selection with dataset of large dimensionality [28]; correlation-based feature selection is effective to handle large-dimensional data with class information [28]. Feature selection is closely connected to data mining and other data processing techniques [27] which will be explained in detail in the experiment section of this work. CFS also employ the use of best-first search algorithm as its strategies to select the best feature set that will improve classification accuracy. The pseudo code for the algorithm is giving in figure 2. The choice of correlation-based feature selection for this work is because of large dimensionality of NSL-KDD and CICIDS 2017 dataset.

To accomplish the goal of this paper, feature selection were carried out on the dataset. The Correlation-based Feature Selection (CFS) is used in this paper. Experiments are performed on a Windows 8.1 Machine (Intel Pentium 2.4GHZ, 6 GB RAM). WEKA tool is used to run CFS on the dataset. The models for the intrusion detection system were built using each of the algorithms; ClonalG, AIRS1 and Immunos1 with wekaclassalgos software. In the case of DCA, Matlab was used in implementing the algorithm. These models were used for predicting the labels of the test data. Feature selection could lead to further improvements in detection rate and complexity. Correlation-based feature selection evaluates the worth of a subset of attributes by considering the individual predictive ability of each feature along with the degree of redundancy between them.

For the NSL-KDD dataset, the features selected by the CFS are Flag, src_bytes,dst_bytes, logged_in, srv_serror_rate, diff_srv_rate and class. The selected features has the highest correlation among other features in the dataset. In the case of the CICIDS dataset, the features selected varied from one attack category to the other. In DOS/DDOS attack, timestamp and init_win_bytes_forward features are chosen. This is also to say that for the simulated DOS/DDOS attack, the selected features has the highest correlation. For botnet, DestinationPort, Bwd_Packet_Length_Mean, Bwd_Packet_length_std and min_seg_size_forward. Web attack make use of fwd_Packet_length_Mean, Fwd_IAT_Min and Init_win_bytes_backward(refer to Table 5).

CFS uses a best-first search algorithm to evaluate the merit of feature subsets. Best-first search explores a graph by expanding the most promising node chosen according to a specified rule. The heuristic by which CFS measures the usefulness of individual features for predicting the class label along with the level of inter-correlation among them. The hypothesis on which the heuristic is based can be stated: Good feature subsets contain features highly correlated (predictive of) with the class, yet uncorrelated with (not predictive of) each other. The Heuristic “merit” for subset *S* is mathematically expressed as:

$$Merit_s = \frac{k\overline{r_{ca}}}{\sqrt{k + k\left(k-1\right)\overline{r_{aa}}}}$$

Where *k* is the number of attributes

$\overline{r_{ca}}$ is the average class-attribute correlation

$\overline{r_{aa}}$ is the average attribute-attribute correlation

where MS is the heuristic “merit” of a feature subset S containing k features, of how predictive of the class a set of features are; the denominator of how much redundancy there is among the features.

```
1. Begin with the OPEN list containing the start state, the CLOSED list empty,and BEST start state.
2. Let s = arg max e(x) (get the state from OPEN with the highest evaluation).
3. Remove s from OPEN and add to CLOSED.
4. If e(s) _ e(BEST), then BEST   s.
5. For each child t of s that is not in the OPEN or CLOSED list, evaluate and add to OPEN.
6. If BEST changed in the last set of expansions, goto 2.
7. Return BEST.
```

Figure 5 : Best –Search Algorithm

The feature selection process for dendritic cells algorithms is a way of selecting signals for the input of the algorithms.

Table 2: Signal Selection for Dendritic cells algorithms for NSL KDD Dataset

Signals	Selected Features
Pamp	2,4,8,10,14,16,18,20,22,24,27,33,35,38,40
Danger	4,5,6,12,26,30,42
Safe	1,3,7,9,11,13,15,17,19,21,23,26,29,32,34,36,39

4.0 RESULTS

This section presents the classification performance of AIRS1, ClonalG , Immnos1 and Dendritic cells algorithms on the dataset used. 10-fold cross validation is applied on both dataset. 10-fold cross validation process divides the dataset into 10 part, nine parts were used as training data and one part was used for testing. The following results were identified for the algorithms using accuracy, precision and recall.

Table 3: CLONALG Classification of CICIDS 2017 Dataset

S/N	Attack	Accuracy %	Time(s)	Precision	Recall	F-Measure	RMSE
1.	DDOS	75.55	21	0.71	0.76	0.73	0.49
2.	Botnet	98.97	33	1.0	0.99	0.5	0.09
3.	Web attack	100	26	1.0	0.99	0.5	0.08
4.	Infiltration	99.9	123.54	1	1	1	0.05
5.	Port scan	61.84	52.86	0.618	0.621	0.618	0.56

Table 3 shows Accuracy, Time taken, Precision, Recall, F-Measure and RMSE of the ClonalG in identifying intrusion. Based on the results shown in the Table 2, it can be identified that ClonalG achieved 100% accuracy in web attack for CICIDS 2017 dataset. Whereas ClonalG has the lowest accuracy on DDOS, Botnet attack has a good detection accuracy with ClonalG.

Table 4: Immunos1 Classification of CICIDS 2017 Dataset

S/N	Attack	Accuracy %	Time(s)	Precision	Recall	F-Measure	RMSE
1.	DDOS	66.68	0.33	1	0.35	0.59	0.43
2.	Botnet	65.67	0.12	1	0.64	0.67	0.59
3.	Web attack	63.3	0.22	1	0.63	0.77	0.43
4.	Infiltration	86.9	4.71	1	0.869	0.93	0.3625
5.	Port scan	63.39	4.12	0.8	0.7	0.6	0.57

Table 4 shows Accuracy, Time taken, Precision, Recall, F-Measure and RMSE of the Immnos1 in identifying intrusion. Based on the results shown in the Table 3, it can be identified that Immunos1 doesn't show good accuracy performance on all the attacks.

Table 5: AIRS1 Classification of CICIDS 2017 Dataset

S/N	Attack	Accuracy %	Time(s)	Precision	Recall	F-Measure	RMSE
1.	DDOS	97.73	1.3	0.99	0.98	0.98	0.15
2.	Botnet	97.78	260	0.99	0.98	0.98	0.18
3.	Web attack	97.90	58	0.99	0.98	0.98	0.12
4.	Infiltration	98.9	193.54	1	0.87	0.95	0.21
5.	Port scan	62.93	123.67	0.75	0.7	0.65	0.59

Table 5 shows Accuracy, Time taken, Precision, Recall, F-Measure and RMSE of the AIRS1 in identifying intrusion. Based on the results shown in the Table 3, it can be identified that AIRS1 show best accuracy performance on all the attacks.

Table 6: DCA Classification of CICIDS 2017 Dataset

S/N	Attack	Accuracy %	Time(s)	Precision	Recall	F-Measure	RMSE
1.	DDOS	81.5	131	0.82	1	0.99	0.39
2.	Botnet	99	260	0.99	1	1	0.08
3.	Web attack	98.7	581	0.9	1	1	0.09
4.	Infiltration	100	393.54	1	1	1	0.49
5.	Port scan	55.5	623.67	0.55	0.7	0.55	0.08

Table 6 shows Accuracy, Time taken, Precision, Recall, F-Measure and RMSE of the Dendritic cells algorithms in identifying intrusion. Based on the results shown in the Table , it can be identified that DCA show best accuracy performance on all the attacks except for Port Scan attack.

The accuracy performance of AIRS1, Immunos1, ClonalG and Dendritic algorithm has been compared to each other on DDos, botnet, web attack, infiltration, and port scan. The comparison for CICIDS 2017 dataset has been shown in Figure 3. Figure 1 also shows the comparison of AIRS1, Immunos1, ClonalG1 and dendritic cells algorithms accuracy performance on NSL-KDD dataset (Refer to Figure 3). For the NSL-KDD dataset, dendritic cells algorithms performs best.

Table 7. Features Selected for each attack of CICIDS 2017 Dataset using CFS

S/N	DOS	Web Attack	Bot net	Infiltration	Port scan
1.	1 Flow ID	2 Source IP	1 Flow ID	11 length of fwd packets	16 Fwd packet length
2.	7 Timestamp	1 Flow ID	5 Destination Port	78 Active Std	76 min-seg-size-std
3.	3 Source Port	74 Init_Win_bytes_backward	4 Destination IP	80 Active Min	80 Active Mean

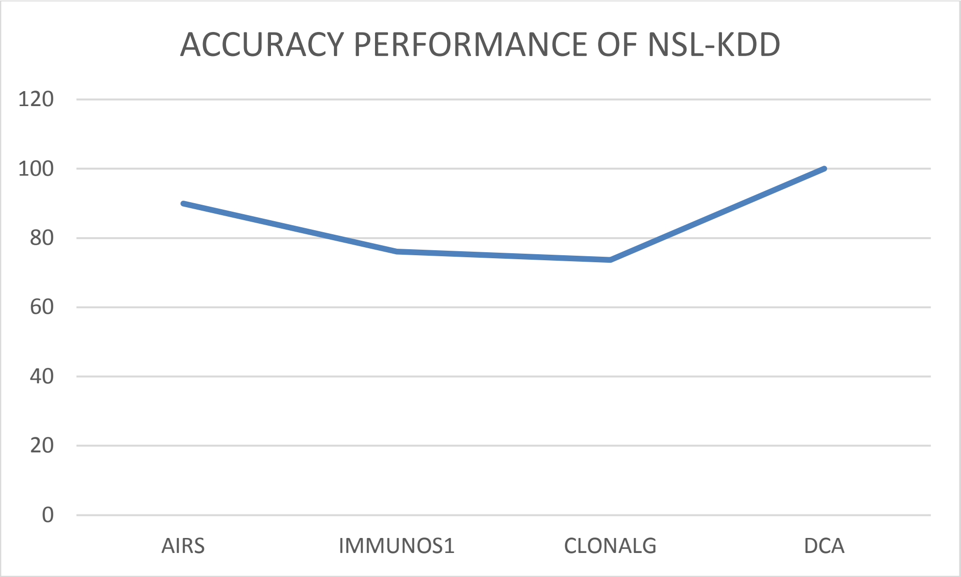


Figure 3 : Accuracy Graph for NSL-KDD dataset

Table 6: NSL-KDD Dataset Classification using Correlation-based Feature Selection CSF

S/N	ALGORITHMS	Accuracy %	Time (s)	Precision	Recall	F-Measure	RSME
1.	CLONALG	89.93	24	0.92	0.9	0.91	0.2
2.	IMMUNOS 1	76.12	0.2	0.66	0.9	0.91	0.4
3.	AIRS 1	73.71	284	0.72	0.6	0.69	0.3
4.	DCA	100	492	1.0	1.0	0.9	0.1

Some of the classifiers used other than AIS based classifiers for comparison of classification accuracy in our experiment are:

ZeroR: ZeroR is the simplest classification method which depends on the target and ignores all predictors. ZeroR classifier simply predicts the majority category (class). It is used for calculating baseline accuracy as a benchmark for other classification methods.

J48: The J48 algorithm is WEKA's implementation of the C4.5 decision tree learner.

The algorithm uses a greedy technique to include decision trees for classification and uses reduced error pruning.

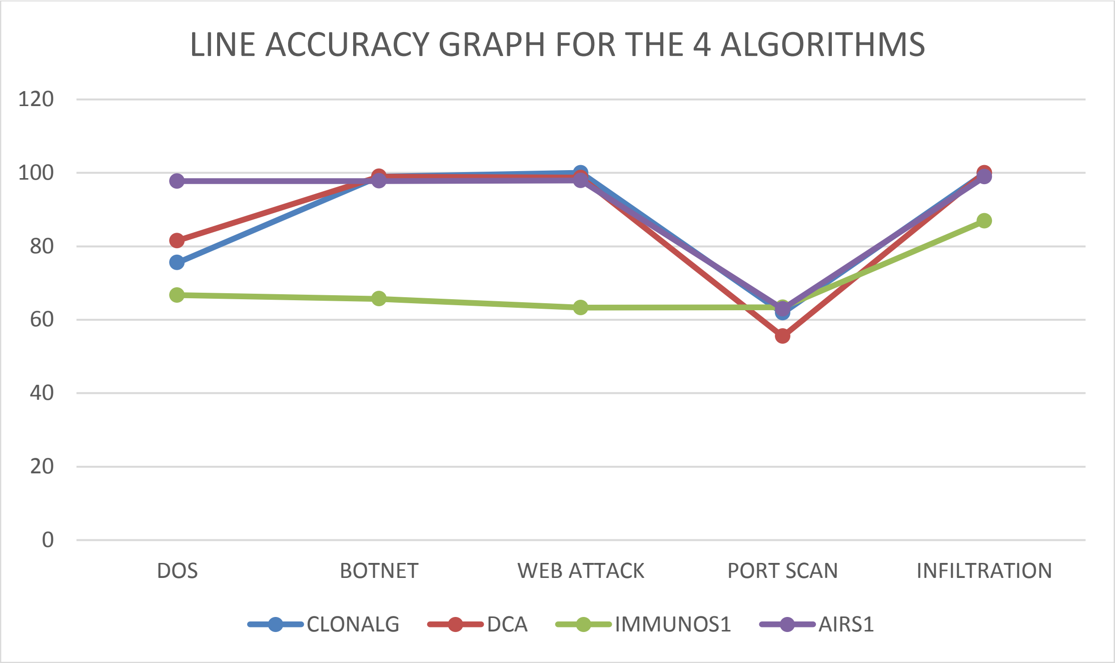


Figure 5: Line Accuracy Graph for 4 Algorithms of the CICIDS Dataset

We found that the level of detecting classification accuracy, sensitivity, F-measure and specificity varied in each dataset but the highest results are seen in the case of AIRS1 algorithm. AIRS1 performed best among all the other AIS algorithms in all the attack for CICIDS 2017 dataset followed by Dendritic cell algorithms. The accuracy performance of all the algorithms are clearly shown in Figure 5. We compared our results with proven classifiers that have performed well on intrusion detection system. We choose ZeroR and J48 classifiers to compare with these AIS algorithms. In our comparison of AIS algorithms with ZeroR and J48 classifier, ZeroR and J48 classifier build their models faster than any of the AIS algorithms but perform poorly in accuracy on CICIDS 2017 dataset. Among the AIS algorithms, ClonalG has the highest number of accuracy using the NSL-KDD dataset for intrusion detection classification while AIRS1 has the highest number of accuracy using the CICIDS 2017 dataset for intrusion detection. Table 3 show the classification performance using CLONALG and Table 4 show classification performance using Immunos1.

In the use of CICIDS dataset, the more features you select, the more time taken to build the models especially for the AIS algorithms. Limited and best feature set also affects the accuracy of AIS algorithms.

5.0 CONCLUSION

Developing a reliable intrusion detection system that can detect common and up-to-date attacks is one of the fundamental concerns of researchers and IDS developer. In this study, effectiveness of 2 different real time intrusion detection dataset using AIS techniques was comparatively evaluated and the results were presented. We also investigated which among of

AIRS1, ClonalG , Immunos1 and dendritic cell algorithms gives a better classification accuracy on common updated intrusion attacks over the network.

Experimental results suggested that, in the detection of updated malicious attacks, the proposed AIS techniques perform better than other classifiers and AIRS1 and DCA performs best on all the dataset in all the cases. In the future, we plan to negative Selection Algorithms and Clonal selection algorithms to evaluate the effectiveness of our AIS classification model on NSL-KDD and CICIDS 2017 dataset.

REFERENCES

[1] Oladayo Tosin Akinwande & Muhammad Bashir Abdullahi. Perfromance evaluation of artificial immune system algorithms for intrusion detection using NSL-KDD and CICIDS 2017 dataset. Proceedings of the 12th International Multi-Conference on ICT Application pp. 140-146 Jugal Network Traffic Anomaly

[2] Bhuyan, Monowar H, Bhattacharyya, Dhruba K, Kalita Jugal Network Traffic Anomaly Detection and Prevention : Concepts, Techniques and Tools Retrieved on http://www.springer.com/gp/book on 19/08/2018 @1:23pm

[2] Ezat Mahmoud Soleiman & Abdelhamid Fetanat . Intrusion detection System using supervised learning vector quantization,
International Journal of Innovative Research in Advanced Engineering Volume 1(10), 2014, 20-25.

[3] Megha Aggarwal Amrita .Performance Analysis of Different Feature Selection Methods in Intrusion Detection. Retrieved from http://www.ijstr.org/finalprint/june2013 on 17/08/2018 @ 12:35am

[4] Kasthurirangan Partgasarathy. Clonal Selection method for immunity based intrusion detection system, Project Report(2014), 1-19

[5] Merim Zekri, Labiba Souici Meslati. Artificial Immune System for Intrusion Detection

[6] Feng Gu, Julie Greensmith, Uwe Aicklein. Further Exploration of the Dendritic Cell Algorithm: Antigen Multiplier and Time Windows LNCS, vol. 5132, pp. 142-153. Springer, Heidelberg (2008)

[7] Jason Brownlee. Clever Algorithms Nature-Inspired Programming Recipes, Revision 2, 16, June 2012 ISBN: 978-1-4467-8506-5.

[8] Hiren K. Mewada and Sanjay Patel. Advances in Intrusion Detection Algorithms for Secure E-business Using Artificial Intelligence. Retrieved from **http://www.scialert.net/fulltext/?doi=rijit.2017.1.6 on 17/08/2018 @ 12:38am**

[9] Jason Brownlee. Clonal Seleciton theory and ClonalG: The Clonal Selection Classification Algorithm, Technical Report No, 2-02, January (2005)

[10] Junyuan Shen and Jidong Wang . An improved artificial immune system based Network intrusion detection by using rough set" Journal of communication & Network Vol. 4 1 in February 2012, 59-63.

[11] Manu Bijone . A survey on Secure Network: Intrusion Detection & Prevention Approaches , American Journalof Information Systems, 2016, Vol. 4(3), 69-88

[12] Gharib A Sharafaldin, I Habibi Lashkari and Ghorbani A.A. An evaluation framework for intrusion detection dataset.

[13] Iman Sharafaldin, Arash Habibi Lashkan and Ali A. Ghorbani .Towards a Reliable Intrusion Detection Benchmark Dataset and Intrusion Traffic Characterisation Proc. 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018

[14] Sanghmitra Dash, Rabindra Kishore Mishra, Rama Krusha Das and Manisha Panda. Comparison of Classifier Outputs using AIS and Non-AIS Based Data Mining Algortihms, International Journal of Artificial Intelligence and Knowledge Discovery Vol. 6, Issue 4, Oct, 2016.

[15] Julie Greensmith, U Aickelin, and S Cayzer. Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection. In Proc. of the Fourth International Conference on Artificial Immune Systems (ICARIS-05), pages 153–167, 2005. 14th -17th August 2005, Banff, Alberta, Canada.

[16] Felix T.S Chan, Anuj Prakash, R.K Tibrewal and M.K. Tiwari (2013). Clonal Selection Approach for Network Intrusion Detection Proc. 3rd International Conference on Intelligent Computational Systems (ICICS). Singapore, 2013

[17] Jason Brownlee. Artificial Immune Recognition System (Airs) A Review And Analysis', January 2005, Technical Report No. 1-02.

[18] Manjula C. Belavagi & Balachandra Muniyal . Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection. Procedia Computer Science Volume89, 2016, 117-123

[19] R. Sridevi, Rajan Chattamivelli, E. Kanna. Analysis of Human Immune System inspired intrusion Detection System . International Journal of Computer Science and Information Technologies Vol.2(5), 2011, 2335-2339

[20] Lingjun Meng, Peter van der Putten, Haiyang

Wang. A Comprehensive Benchmark of the Artificial Intrusion Immune Recognition System(AIRS). Proceedings of the first International Conference on Advanced Data mining and application. Retrieved from http://www.semanticscholar.org on 07/09/2018 @ 12:12pm

[21] Andrew Watkins & Jon Timmis . Artificial Immune Recognition System (AIRS): Revisions and Refinements. Retrived from http://www.semanticscholar.org/paper on 16/09/2018 @ 12:14pm

[22] Jayshree Jha and Leena Ragha. Intrusion detection system using support vector machine. International Journal of Applied Information System (IJAIS)-ISSN: 2249-068

[23] Olubadeji Bukola and Adetumbi. Autot-immunity Dendritic Cell Algorithm. International Journal of Computer Applications (0975-8887)Volume 137-No2 March 2016

[24] Obinna Igbe, Ihab Darwish and Tarek Saadawi Deterministic Dendritic cell algorithm application to smart grid cyber-attack detection. Retrieved from http://www.researchgate.net on 30/03/2019 @ 12:01am

[25] Amira Sayed A. Aziz, Ahmad Taher Azar, Mostafa A. Salama, Aboul Ella Hassanien and Sanaa El-Ola Hanfy. Genetic Algortihm with Different feature Selection Techniques for Anomaly Detectors generation Proceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 769-774

[26] Ali Shiravi, Hadi Shiravi, M.T. and Ghorbani, A.A. Toward developing a systematic approach to generate benchmark datasets for intrusion. Computers and Security, 31(3): 357-374

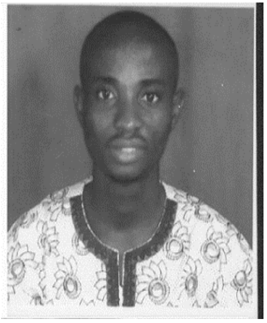
[27] Mcafee (2016).Mcafee labs Threats Report, Retrieved from http://www.mcafee.com/reports on 07/09/2018 @ 12:31pm

[28] You chen, Yang Li, Xue-Qi Cheng and Li Guo (2006). Survey and Taxonomy of Feature Selection Algorithms in intrusion detection system, Inscrypt 2006, LNCS 4318, pp. 153-167, 2006.

[29] Mark A. Hall, Llyod A. Smith (1996). Feature subset selection : A correlation Based Filter Approach. Proc. of International Conferece on neural Information Processing and Intelligent Information System. Berlin: Springer, pp 855-858

Biographies of the Authors.

1. **Akinwande, O.T**



Akinwande, O.T obtained his B.Tech in Computer Science from Federal University of Technology, Minna, Niger State, Nigeria. He is currently a Master Student of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria. He is a member of Nigeria Computer Society (NCS).

2. **Abdullahi, M.B**

Abdullahi, M.B received his B.Tech (Honors) in Mathematics/Computer Science from Federal University of Technology, Minna-Nigeria and Ph.D. in Computer Science and Technology from Central South University, Changsha, Hunan, P. R. China. His current research interests include trust, security and privacy issues in data management for wireless sensor and ad hoc networks, Cloud computing, Big data technology and information and communication security. He is a member of Computer Professionals (Registration Council) of Nigeria (CPN) and Nigeria Computer Society (NCS).