Method for Detecting Anomalies Through Clustering Artificial Immune Networks

Mr. G N VISWESWARA RAO , Mr. KONDAVETI RAJA , JAKKAM SETTI SUNIL BABU
IT DEPARTMENT
Assistant.Professor[1,2,3]
Swarnandhara College of Engineering & Technology,Narsapuram-534275.

Abstract— There are a plethora of Intrusion Detection (IDS) methods available online. It is impossible to use signature-based systems for anomaly detection since they need constant updating with new signatures of unknown assaults. Conversely, anomaly based techniques need a labeled dataset to build the detection profile and have poor detection rates and high false alarm rates. The truth is that it is quite difficult to get a labeled dataset of this type. In this study, we explore the use of an Artificial Immune Network, a clustering method inspired by biology, to identify intrusion detection system clustering assaults. The Rough Set approach was used to extract the most important characteristics from the DARPA KDD Cup 1999 dataset in order to minimize its dimensions. After that, the aiNet clustering technique, developed for Artificial Immune Networks, was used on the modified dataset. Applying the most important traits alone, rather than all of them, improved the detection rate. Further evidence that Artificial Immune Networks are effective in identifying new types of assaults is presented.

***Index Terms*—IDS, Feature Reduction, Artificial Immune Network, Clustering.**

1. INTRODUCTION

As stated in [1], Intrusion Detection Systems (IDS's) are security technologies that aim to enhance the protection of communication and information systems, similar to other measures like firewalls, antivirus software, and access control schemes. Separating the system's typical operations from any other, potentially invasive, aberrations is the primary goal of such technologies.

The literature classifies two basic methods to intrusion detection systems: anomaly detection systems and abuse detection systems. The former looks for out-of-the-ordinary patterns of activity and compares them to typical patterns of conduct in order to spot any changes. On the other hand, the latter relies on predetermined attack signatures and can only identify known attack patterns.

As a pattern recognition challenge, the intrusion detection system (IDS) issue has been the subject of several academic investigations, such as [2,16,18].or, more accurately, as a mechanism for learning. In order to make classification systems simpler and more accurate, it is necessary to remove irrelevant and redundant information from learning systems [2, 17]. In order to meet the demands of accurate and cost-effective IDSs, it is necessary to decrease the representation space of these attributes.

Feature reduction was proposed by Bello et al. in [3] as a means to lower the dimensionality of the training dataset. In addition, they said that feature reduction contributes to faster data processing and better classification rates by lowering the impact of noise.

Based on various machine learning and soft computing methodologies, several anomaly detection systems have been suggested in the literature. Narrowly focused learning methods including neural networks [19], genetic algorithms [20], support vector machines [21], bio-inspired algorithms [22], and countless more are used in certain investigations.

In addition, several IDSs are based on ensemble or a mix of different learning approaches, as discussed in [9, 24, 25]. In specifically, all of these methods have been designed to identify and categorize incoming network traffic as either legitimate or malicious.It is possible to build computational models that draw on the ideas, principles, and processes found in biological systems by drawing inspiration from biology. Methods that draw inspiration from biology include immunological computation, quantum computing, molecular computing, neural networks, and evolutionary algorithms. These bio-inspired systems have recently gained a lot of attention for their remarkable capacity to adapt to their environments. As an example of one such system, the human immune system offers ideas for a broad variety of novel problem-solving challenges [23].

In order to create an anomaly detection system that takes feature reduction into account, this work sets out to do just that. It also included the usage of an AI system that is bio-inspired to identify new assaults that weren't there in the training data.

The rest of the paper is organized as follows. Section 2gives a view on the methods used in this study which are rough set and artificial immune network. Section 3 describes some related works in both areas namely, feature reduction and unsupervised immune network for clustering. In section 4, the experiments using KDD CUP 99 dataset are shown. It also includes an analysis of the results and performance comparison against k-Means method. We conclude the paper in Section 5.

I. BACKGROUND

A. Rough Set Theory

Rough Set can be defined as a mathematical tool for approximate reasoning for decision support and isparticularly well suited for classification of objects [4]. It has been stated that, this tool can also be used for feature reduction and feature extraction. The most attractive characteristics of rough set is that it deals with inconsistencies, uncertainty and incompleteness of data instances by determining an upper and a lower approximation to set membership. It has been successfully used in the literature as a selection tool to discover data dependencies, find out all possible feature subsets, and remove redundant information. More theoritical definitions about rough eet can be found in [5].

B. Artificial Immune Network

Immune network theory has been proposed first by Jerne in [6] and it has been widely used in the development of Artificial Immune System (AIS) [7]. Thistheory suggests that for each antibody molecule, there isa portion of their receptor that can be recognized by otherantibody molecules. As the results, a network communication can occur within the immune system, andit is called as Immune Network.

Network activation and network suppression are two important characteristics of immune network. According to de Castro and Timmis [8], the recognition of antigen by an antibody results in network activation, whereas the recognition of an antibody by another antibody results in network suppression. The antibody Ab_2 is said to be the internal image of the antigen Ag, because Ab_1 is capable of recognizing the antigen and also Ab_2. According to the Immune Network theory, the receptor molecules contained in the surface of the immune cells present markers, named idiotopes, which can be recognized by receptors on other cells [8]. Fig.1 below gives a view about the immune network.

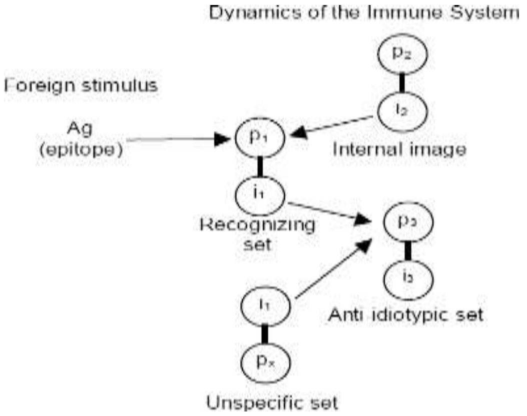

Figure 1. A view on idiotypic Immune Network [8]

One way to learn that doesn't need human oversight is via an Artificial Immune Network. A model of an artificial immune system is an antibody-like collection of cells linked together by linkages of varying strengths. In their networked form, these antibodies stand in for the network's internal representations of pathogens existing in their surroundings, which are input patterns. The Immune Network aiNet algorithm is detailed below:

1. Import the population of antigens.
2. As a seed for each cluster, randomly choose one antigen from the antigen population to initialize the Immune Network.
3. Even if it is not true that the termination condition:

a. I. Introduce an antigen to the network for every antigen pattern in the antigen population
ii. Find out how well each antibody cluster binds to the antigen.
iii) From the network, choose the n antibodies with the greatest affinity. iv) For each of these antibodies, do the following:
The condition where its affinity exceeds the affinity threshold d σ is met.
After that.
a. Appropriately replicate the antibody based on its affinity
b. Mutations occur in clones at a rate inversely proportionate to their affinity.
c. Make those antibodies more effective
Section v concludes with Section vi.In the event that not a single high-affinity antibody was able to bind the antigen, you may use it to start a new cluster.
b) Exit from
c. Suppress after calculating the antibody-antibody affinity inside each cluster.
d. Figure out how well cluster-cluster and do suppression work together.
Deleting the antibodies from every cluster when the fitness falls below a certain threshold f σ is the next step.

4. Finish
5. Provide output for every network cluster.
6. Express every network cluster

Companion Tasks

A. Making Intrusion Detection Systems with Fewer Features

In order to identify intrusions, most intrusion detection systems (IDSs) in the literature look at every aspect of the dataset. Actually, it's possible that certain characteristics are superfluous or don't add anything to the detection at all. In order to make our suggested model more efficient and successful, we need to find the key input characteristics in the IDS dataset that help with detection. This is the goal of this part of the research.

Two feature reduction techniques, one using Bayesian networks (BN) and the other using Classification and Regression Trees (CART), were studied by Chebrolu et al. in [9]. Furthermore, they looked at BN and CART ensembles as well. Their findings highlighted the significance of feature reduction in developing efficient and effective intrusion detection systems for use in the real world. Zhang et al. investigated Rough Set's potential for feature reduction in [4]. Their research proved that this program can retrieve the rules for categorizing attacks in IDS. There was a lack of transparency on the characteristics used for classification.

Data reduction may be accomplished by several means, such as filtering, data clustering, and feature selection, as stated in [9]. According to the authors in [10], one of the main problems with anomalous intrusion detection is that it can't always tell the difference between regular and abnormal activity. Furthermore, this research also noted that network traffic data is massive, leading to excessively high overhead and often posing a significant challenge in intrusion detection systems. Along with that, they proved that IDS performance was unaffected by removing these superfluous elements.

Machine learning and pattern classification algorithms' ability to identify assaults is often impacted by the presence of these superfluous and superfluous elements, according to Chakraborty in [11]. Improved classification performance was shown by Hassan et al. in [12] as a consequence of carefully choosing the feature set.

Clustering Immune Networks (B)

The real value of intrusion detection systems (IDSs) lies not in their capacity to address the massive amount of known vulnerabilities, but in their capacity to discover an unknown quantity of vulnerabilities that may not be immediately accessible to experts for analysis and incorporation into the database of knowledge [13]. To address this need, the authors of [13] presented a clustering-based unsupervised anomaly detection system. According to their claims, this method can identify more types of previously unseen assaults.

Manually classifying data is costly and time-consuming, therefore labelled or otherwise normal data is usually not easily accessible. Similarly challenging to achieve in reality is data that is completely typical, since it is quite difficult to

to automatically adjust and group typical and malicious data without any background information.

II. PROCEDURES AND OUTCOMES

To begin, we will describe the dataset that has been utilized to verify our method. Our experimental strategy for implementing our concept is then shown. We used the rough set tool to decrease the dataset's characteristics in the first phase of the two-part trials. In the second step, immunity network clustering, normal data from assaults is clustered using the feature subset acquired from the previous phase as input.

I. List of records

For the purpose of validating the suggested technique, the dataset chosen is KDD Cup 1999. In order to measure the efficacy of intrusion detection methods, several researchers utilize this standard dataset.

There are 4,940,000 entries in the original dataset, which has 744 MB of data. But, in order to perform experiments on this dataset, the majority of researchers have only worked with a tiny subset of it (10 percent). Forty-94,021 records make up 10% of the total. Each connection record in the dataset includes 41 characteristics, including one class label. Differentiating between legitimate connections and malicious ones is made easier with the help of derived characteristics. Nominal or numerical characteristics describe these traits.

Attacks on the KDD CUP dataset fall into one of four broad types. Following here is a synopsis of each lesson.

One kind of assault is known as a denial-of-service attack, and it involves flooding a computer or memory resource to the point that it can't handle any more requests.

For example, in a probing attack, the perpetrator probes the target network in search of security flaws.

• Hackers may get root access to a system by gaining access to a regular user account. This kind of assault is known as a "user to root" attack.

An attacker may learn about a system's possible weaknesses by sending packets to it remotely across a network; this kind of attack is known as a Remote to User Attack.

Using ROSETTA for Feature Reduction (B)

Three independent dataset samples, each with 10,000 occurrences, are used to validate our suggested methods. Data distribution and class counts are shown in Table 1 for these samples.

to make sure nobody gets in while they were

The first table

amassing data from networks [14]. Therefore, a bio-inspired method is suggested as a means to tackle these issues: an unsupervised anomaly detection strategy based on artificial immune networks.

HE DISTRIBUTION OF ATTACKS IN THE DATA SAMPLES

Normal	**Probe**	**DoS**	**U2R**	**R2L**
2000	684	6907	34	375

The data samples are subjected to rough set after their production. Ohrn created the ROSETTA system (Rough SET Toolkit for data Analysis) to implement Rough Set [15].

The steps of the experiment are as follows: Initially, ROSETTA-recognized Tables are created from the raw data samples. Following the data samples' preparation, they are divided into two parts: the training dataset and the testing dataset. The splitting factor is something the user decides upon; for example, a split factor of 0.4 would divide the data samples into 40% for training and 60% for testing.

A number of techniques, such as GA, Johnson Holte1R, and dynamic algorithms, may be used to decrease the number of data samples. In order to simplify the data sample for this investigation, the GA method is used. We are intrigued by GA since, as stated by Ohrn [15], it is used to discover minimum hitting sets and produces less reductions than Johnson's method.

The GA built-in algorithm in the ROSETTA tool is used to produce the rules using the collection of reducts acquired in the third stage. The second portion of the data sample, the testing portion, will be classified later on using these criteria.

Following a series of tests, the following table displays the eight most important attributes.

TABLE 2
THE MOST 8 SIGNIFICANT FEATURES OBTAINED BY ROUGH SET IN THREE DIFFERENT SAMPLES OF DATA.

Data Sample	**8 most significant features**							
Sample 1	C	E	F	Y	AD	AF	AG	AI
Sample 2	C	E	F	W	AG	AF	AH	AJ
Sample 3	C	E	F	Y	W	AE	AI	AN

Table 2 it seems that all samples had three characteristics in common, with the remainder varying in frequency. Each and every one of the examples shares features C, E, and F. Both samples have the characteristics AF and AG. The third example shares features AI and Y with the first. I often see feature W.TABLE 4
THE CORRESPONDING NETWORK FEATURES AND THE DESCRIPTION OF THE FEATURES FOR THE OBTAINED FEATURES

Feature label	**Corresponding Network Feature**	**Description of feature**
C	Service	Type of service used to connect (e.g. fingure, ftp, Telnet, SSh, etc.).
E	Src_bytes	Number of bytes sent from the host system to the destination system.
F	Dst_bytes	Number of bytes sent from the destination system to the host system.
W	Count	Number of connections made to the same host system in a given interval of time
AF	Dst_host_count	Nnumber of connections from the same host to destination during a specified time window.
AG	Dst_host_srv_ count	Number of connections from the same host with same service to the destination host during a specified time window.

AI	dst_host_diff_srv_rate	Number of connections to different services from a destination host.

In order to compare the performance of the rough set classifier both before and after feature reduction, it was used for data classification in addition to feature reduction. The following table displays the outcomes.

in comparison to samples 2 and 3. In light of this shared characteristic, we identified eight crucial

Type		Sample 1	Sample 2	Sample 3	Mean	StDv
Normal		92.8%	95.2%	79**%**	92%	0.04
Attack	Prob	94.3%	100%	99.3%	97.9%	0.03
	DoS	99.9%	99.9%	100%	99.9%	0.00
	U2R	46.7%	66.7%	26.7%	46.7	0.20
	R2L	92.5%	84.3%	94%	90.2	0.05

TABLE 5
THE CLASSIFICATION ACCURACY OBTAINED BY ROUGH SET ON THREE DIFFERENT SAMPLES USING ALL 41 FEATURES.

features in the three samples and in the whole dataset are shown in the following table.

TABLE 3
THE MOST 8 SIGNIFICANT FEATURES OBTAINED BY ROUGH SET

C	E	F	W	Y	AF	AG	AI

The corresponding network features and the descriptionof each feature are shown in table 4.
Table 5 displays the outcome of data sample classification utilizing all 41 characteristics of the dataset. We can see the misclassification of the unbalanced classes U2R and R2L in the table. We categorized the data utilized in this research into samples to retain the original distribution as in the main dataset since these classes are infrequent and their ratio is extremely tiny in the main KDD CUP 99 dataset.

To test how feature reduction affected the results, we ran the rough set classifier on both the full-featured and reduced datasets using the same data samples.TABLE 6
THE CLASSIFICATION ACCURACY OBTAINED BY ROUGH SET ON THREE DIFFERENT SAMPLES USING ONLY THE 8 MOST SIGNIFICANT FEATURES.

Type		Sample 1	Sample 2	Sample3	Mean	StDv
Normal		93.2%	97.5%	88.8%	93.2%	0.643
Attack	Prob	95.5%	94.7%	96.4%	95.5%	0.008
	DoS	99.4%	99.7%	99.3%	99.4%	0.002
	U2R	34.3%	66.7%	80%	60.3%	0.235
	R2L	85%	84.9%	99.3%	90%	0.082

Looking at the results of the sample categorization using just the eight most important characteristics reveals that certain classes see no significant drop in accuracy while others see an improvement. This is due to the fact that many examples belonging to the most data-intensive classes (such as Normal and DoS) include redundant attributes that are not useful for instance detection.

Furthermore, there is less correlation between the characteristics in these cases. Consequently, the classifier's performance in these classes was unaffected by the feature reduction method. Cases in other classes, known as unbalanced classes, include characteristics that are noisy and uncorrelated, which impacts the accuracy of classification. In addition, the data space hosts assaults that are uncommon in these classes. By removing characteristics that aren't connected to each other, the feature reduction method helps the classifier perform better.

Figure 2 below shows a comparison between the characteristics chosen by Chebrolu et al. in [9] using the Bayesian Networks technique (BN) and the features generated by our model. We discovered that eight of the twelve traits chosen for their research—C, E, F, L, W, X, Y, AB, AE, AF, AG, AI—were also chosen for our investigation.

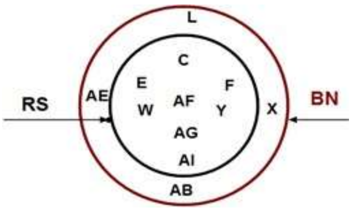

Figure 2. A comparison with BN approach in [9].

The Immune System Artificial intelligence-based clustering

This step involves testing the aiNet algorithm's capability to cluster various types of data using the same data samples that were used for feature reduction using rough set. You can see the breakdown of assaults and normal occurrences in these data samples in Table 7.

TABLE 7

THE DISTRIBUTION OF THE NORMAL AND ATTAK INSTANCES INDATA SAMPLES

Sample/Class	Normal	Probe	DoS	U2R	R2L
All samples	2000	684	6907	34	375

The normalization technique is conducted before the data samples are input into the immune network model. Both numerical and nominal characteristics are included in the KDD CUP'99 dataset. The nominal qualities are transformed into linear discrete values (integers) by the process of normalizing. The "ftp" protocol is denoted by 1 and the "http" protocol by 2, for instance. The characteristics might be either discrete-valued features or continuous-valued attributes. A feature's ability to dominate the others depends on its range. There are a plethora of normalizing techniques available, such as the Mean/Median Scaling approach and distance-based methods.

After setting up the parameters of the aiNet algorithm such that (N*gen*= 10, σ_d =1, σ_S =0.3, Percentile amount of clones to be re-selected=10, and the learning rate=0.4),and applying it on the data samples, the results are shownin Table 7.

TABLE 8

CLUSTERING RESULTS OBTAINED BY AINET CLUSTERING

Sample/Class	**Normal**	**Probe**	**DoS**	**U2R**	**R2L**
Sample 1	3580	1598	4776	9	37
Sample 2	3495	640	5823	6	36
Sample 3	3420	1590	4949	5	36

Results from aiNet-based clustering of data samples into five groups, with one group representing each data type, are shown in Table 8. The data distribution differs from the result clusters for each class, as seen in Table 7. Every clustering approach does this; it's based on the distances between data instances, and in our dataset, both regular traffic and assaults share commonalities. Because of these shared characteristics, distinguishing between typical and malicious cases is challenging.

One way to display the findings from Table 8 is in a binary classification format, such in Table 9, which separates the data into normal and abnormal (attack) categories.

TABLE 9

THE RESULT OF CLUSTERING DATA SAMPLES IN TWO CATEGORIES (NORMAL AND ANOMALIES)

Sample/Class	**Normal**	**Anomalies (attacks)**

Sample 1	3580	6420
Sample 2	3495	6505
Sample 3	3420	6580

Finding the detection rate (DR) and the false positive rate (FPR) is where binary-classification representation really shines. Based on our studies on three sample sets, Table 10 displays DR and FPR.

TABLE 10

DETECTION RATE AND FALSE POSITIVE RATE FOR THE CLUSTERING PROCESS DONE BY AINET ALGORITHM

Sample/Class	**Detection Rate**	**False Positive Rate**
Sample 1	80.25%	0.1975
Sample 2	81.31%	0.1868
Sample 3	82.25%	0.1775

The relation between FPR and DR can be expressed using the ROC curve. The following Figures show the ROC curves for sample1 of the dataset.

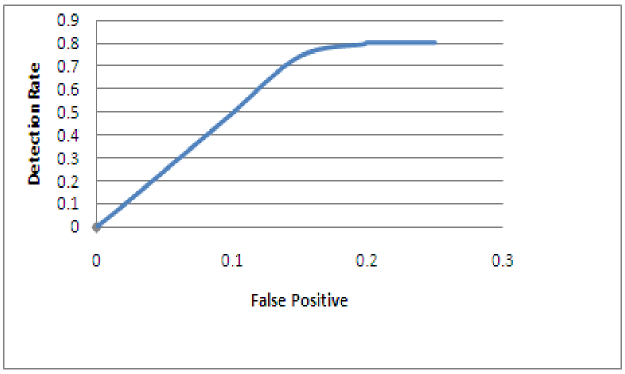

Figure 3. ROC curve for sample1

As we shall see in the study that follows, Figure 3 shows that the FPR is much lower than other intrusion detection methodologies. These findings suggest that aiNet is capable of differentiating between malicious and benign traffic. Cluster assaults may be executed using aiNet even when labels and background information are not available.

The effectiveness of aiNet was further assessed by contrasting it with k-Means, a widely used clustering technique in several domains, including intrusion detection. Using the same data samples, we have used the k-Means technique. All k clusters had their seeds randomly selected before running k-Means, where k is the number of clusters.

The K-Means method's ROC curve is shown in the image below. It illustrates the connection between DR and FPR.

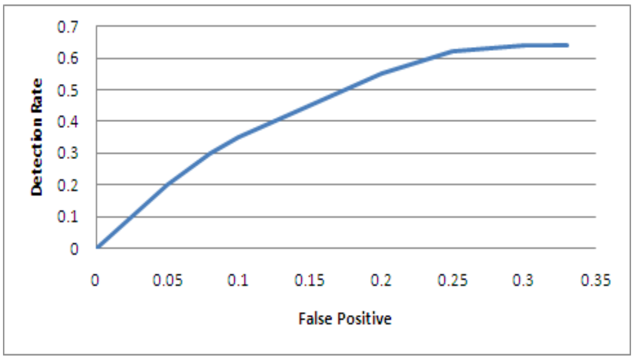

Figure 4. ROC curve for sample1 of group 2 using K-Means.

K-Means seems to have a low DR and a high FPR in Figure 4. This is because intrusion detection data is inherently biased, with commonalities among instances from various classes and an uneven distribution of assaults across them. Also, the findings show that k-Means, which uses distance measurements a lot, did a bad job of clustering the data.

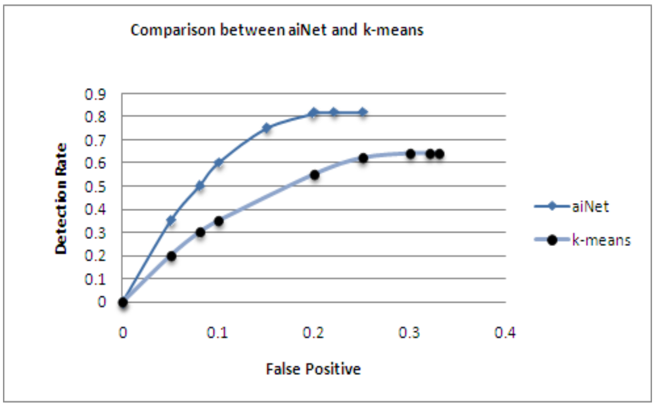

Figure 5. The comparison between the ROC curves of both aiNet and K-Means methods for the same data sample.

To illustrate aiNet's performance in contrast to k-Means, we provide the ROC comparison between the two algorithms in Fig. 5. When comparing DR with FPR, we find that aiNet outperforms K-Means.

Additional research into the aiNet features has shown that aiNet is sufficiently efficient at data compression. At the completion of the clustering process, aiNet creates output cells, and Figure 6 below depicts the tradeoff between these cells and the suppressing threshold □S.

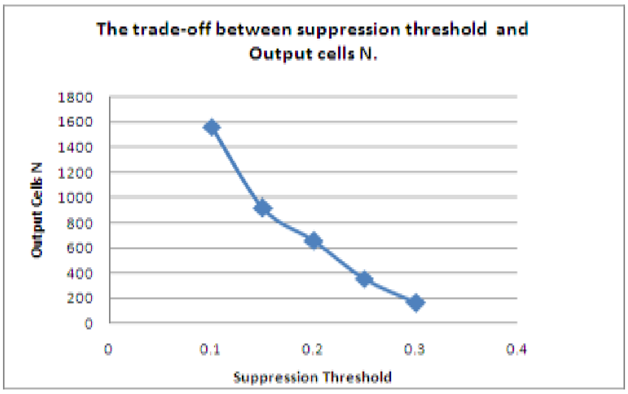

Figure 6. The tradeoff between the suppression threshold and the number of output cells produced by aiNet.

Fig. 6 shows that, beside the ability of aiNet in clustering attacks, it has also the ability to compresses the dataset which make it more suitable for large scale datasets.

II. CONCLUSION AND FUTURE WORK

Using an appropriate feature reduction tool improves detection accuracy and decreases false alarms in intrusion detection systems, according to this research. Furthermore, a bio-inspired immune network clustering method may identify new, undiscovered assaults that were not present during training. Using a rough set for feature reduction enhanced detection accuracy, according to the testing data. At the same time, the AINet clustering algorithm has solved the issue of discovering new assaults. We compared our method to the k-Means clustering method to demonstrate its feasibility; the findings revealed that our method outperformed the other in terms of the accuracy with which it detected new assaults. The results also demonstrate that the Immune Network clustering method may effectively identify new assaults even when labels are not available.Our future work will include the automated setup of aiNet's settings to simplify its operation. To further improve detection accuracy, future research should investigate the feasibility of switching from an unsupervised to a semi-supervised clustering strategy by adding labels to the existing data.

REFERENCES

G. Macia'-Ferna'ndez, E. Va'zquez, J. Dıaz Verdejo, and G. Teodoro are the authors of the cited work. "Methods, systems, and challenges for anomaly-based network intrusion detection" Pages 18–2 of the March 2009 edition of Computers and Security, volume 28, issues 1-2.

S. Shamduddin, M.A. Maarof, and A. Zainal [2]. In the 2006 IEEE TENCON proceedings, the author discusses "feature selection using rough set in intrusion detection" on page 4.

[3] "A Model Based on Ant Colony System and Rough Set Theory to Feature Selection" by R. Bello, Y. Caballero, Nowe, Y. Gomex, and P. Vrancx. pp. 275-276, June 25-29, 2005, in GECCO'05, Washington DC, USA.

Intruder Detection Using Rough Set Classification was published by L. Zhang, G. Zhang, L. Yu, J. Zhang, and Y. Bai in 2004. Volume 10, Issue 4, Pages 1076–1086, Journal of Zheijiang University Science, 2004.
[5] "Rough Sets: Theoretical Aspects of Reasoning about Data" by Z. Pawlak. Published by Kluwer Academic in 1991.
"Network theory of the immune system." 1974. Annals of Immunology, Paris, [6] Jerne, N.K.
"Artificial immune systems as a novel soft computing paradigm" [7] L.N. De Castro, J. Timmis. Soft Computing, 7th Edition, 2003, pp. 526–544, Springer-Verlag.
The authors of this work are De Castro and Timmis (2002). An Artificial Immune Network for Multimodal Function. Paper presented at the 2002 International Congress on Immune Systems, Volume 1, pages 699–704.
A. Abraham, S. Chebrolu, and J.P. Thomas [9]. Intrusion Detection System Ensemble Design and Feature Deduction. Computers and Security: An International Journal, Volume 24, Issue 2, Pages 295–307, 2004.
[10] S. Mukkamala and A.H. Sung. Chapters 468–488 of Springer's 2004 book "The Feature Selection and Intrusion Detection Problems" (LNCS, vol. 3321).
[11] In "Feature Subset Selection by Neuro-rough Hybridization," B. Chakraborty (2005) cites a work published in LNCS by Springer Hiedelberg and spanning pages 519 to 526.
Authors: Hassan, Hasan M.S., Shaharoun A.M., and Jamaluddin H. Statistical Feature-Based Pattern Recognition for SPC Charts: An Improvement. A publication of the International Journal of

Volume 41, Issue 7, pages 1587–1603, published in 2003 by Production Research.
[13] "Solving the Problem of Network Intrusion Detection with Self-Organizing Maps" by S. Zanero. "Clustering High Dimensional Data and its Applications" was the topic of the 2005 SDM Workshop.
Leckie, K., and Leung, C. (2016). Cluster-Based Intrusion Detection for Unsupervised Anomaly Detection in Networks. The University of Newcastle in Australia hosted the 28th Australasian Computer Science Conference in 2005.
[15] "A Rough Set Toolkit for Analysis of Data" by A. Ohrn and J. Komorowski. Volume 3, pages 403–407, 1997, United States of America, in Proceedings of the Third Joint Conference on Information Sciences.
[...] "A Hierarchical Intrusion Detection Model based on the PCA Neural Networks" by G. Liu, Z. Yi, and S. Yang. Page numbers 1561–1568 in the 2007 edition of the International Journal of Neurocomputing.
[17] Mahfuzur Rahman, N. Harbi, and D.M. Farid. For adaptive intrusion detection, "Combining Naïve Bayes and Detection Tree" is the method to use. Journal of Network Security and Its Applications (IJNSA), Volume 2, Issue 2, pages 12–25, 2010.
18. "Research on Immune based Adaptive Intrusion Detection System Model" (L. Deng and D.Y. Gao). On pages 488-491 of the 2009 IEEE International Conference on Networks Security, Wireless Communications, and Trusted Computing.
The paper "Detecting anomalous and unknown intrusions against programs" was written by A.K. Ghosh, J. Wanken, and F. Charron [19]. The 1998 Annual Conference on Computer Security Applications (ACSAC'98) was held in December 1998.
[20] "An SVM-based machine learning framework for detecting network anomalies" (T. Shon, Y. Kim, C. Lee, J. Moon). Workshop on Information Security, IAW'05.2005.
21] D. Kim and J. Park. Using Support Vector Machines for Network-Based Intrusion Detection. On pages 747–756, Springer published their lecture notes in computer science in 2003.
The author is D. Dasgupta."A General Framework for an Immunity-Based Intrusion Detection System." In the proceedings of the 22nd National Instruments Science and Control Conference (1999b).
An Immune Network Approach for Web Document Clustering, by X. Hang and H. Dai [23]. Part of the Proceedings of the Wisconsin Institute of Science, 2004, pages 278–284.
The authors of the paper "An unsupervised network anomaly detection approach by k-Means" are Y. Yasami, S. Khorsandi, SP. Mozaffari, and A. Jalalian. Volume 2008 of the IEEE Symposium on Computers.
Source: [25] Cheng, X., Chin, Y.P., and Lim, S.M. "A dual-level hybrid classifier designed for intrusion detection systems using Bayesian clustering and decision trees (IDS)". In May 2008, Elsevier published a paper in Pattern Recognition Letters, Volume 29, Issue 7, Pages 918-924.