ISSN 2047-3338

A PCA-AIS Approach for Intrusion Detection

R. Sridevi[1], G. Jagajothi[2] and Rajan Chattemvelli[3]

[1]Department of Information Technology, Shri Angalamman College of Engg & Tech, Trichirappalli, India
[2,3]Department of Information Technology, Periyar Maniammai University, Tanjore, India
devivelon@yahoo.com

***Abstract*—Intrusion detection is now a significant part in computer and network security. Various intrusion detection approaches are presented to secure the network, but the performance of the system is reduced. Thus, to improve the detection rates and decrease false alarm rates in intrusion detection is important. The crux of an efficient intrusion detection system is its ability to differentiate between normal and potentially harmful activity. Earlier, developers had used coded rules and blocking specific activities for safeguarding the system. However, in view of the current and future threats, automated and adaptive detection systems are required to safeguard the system. In this paper, an adaptive intrusion system is proposed based on Artificial Immune Systems (AIS). The AIS is based on the Human Immune System (HIS). HIS can detect and defend against harmful and previously unknown invaders, so an Intrusion Detection System (IDS) based on the same principles is proposed. The KDD-cup dataset is used that is a benchmark for evaluating the security detection mechanisms. The Principal Component Analysis (PCA) is applied to transform the input samples into a new feature space.**

***Index Terms*—Intrusion Detection System (IDS), KDD Cup 99 Dataset, Principal Component Analysis (PCA) and Artificial Immune Systems (AIS)**

I. INTRODUCTION

SIMPLY put, intrusion detection systems (IDS) do exactly what their name suggests: they detect intrusions. Specifically, IDS detects computer attacks and/or computer misuse, and alert concerned individuals upon detection. A network with IDS installed works similar to a burglar alarm in a house. Through differing methods, both detect when an intruder/attacker enters and both issue some type of warning/alert. Though IDSs are used along with firewalls, which regulate/control information flow in and out of the network, the two security providers are not the same. Firewalls protect networks and try to prevent intrusions, while IDS tools detect if the network is under attack or has been breached. IDS tools are part of a complete security system. While they do no guarantee security totally, they do enhance network security when used along with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls.

IDS serve three security functions: they monitor, detect, and respond to unauthorized activity both by company insiders and outsider intrusion. IDS define certain events that, when detected leads to an alert. In other words, when a particular event is thought to be a security threat an alert is issued after detection. Certain IDS send out alerts, so that the IDS administrator receives notification of a probable security threat through a page, email, or SNMP trap. Many IDS in addition to recognizing a threat and issuing an alert also respond to the event and this could include logging off a user, disabling a user account or the launching of scripts [1].

Of the many security incidents that take place in a network, the majority (up to 85%) are from within the network. These attacks may include unauthorized users who could be mainly disgruntled employees. The rest are from without and they include denial of service attacks, or attempted penetration of network infrastructure. IDS are the only proactive ways to detect and respond to threats originating from within and without a corporate network [2].

As said earlier intrusion detection is the monitoring computers/networks for unauthorized entrance, activity, or file modification. IDS can also monitor network traffic, to detect if a system is being targeted by a network attack like denial of service attack. There are two basic types of intrusion detection: host-based and network-based and each has a distinct approach of monitoring and securing data, and each has its own advantages and disadvantages. Simply put, host-based IDSs check data in individual computers that serve as hosts, and network-based IDSs check data exchanged between computers.

The efficiency of an IDSs depends on its ability to differentiate between normal and potentially harmful activity. Earlier, developers had used coded rules and blocking specific activities for safeguarding the system. However, in view of the current and future threats, automated and adaptive detection systems are required to safeguard the system. In this paper, an adaptive intrusion system is proposed based on Artificial Immune Systems (AIS). The AIS is based on the Human Immune System (HIS). HIS can detect and defend against harmful and previously unknown invaders, so an Intrusion Detection System (IDS) based on the same principles is proposed. The IDSs is used along with prevention techniques such as encryption and firewalls for safeguarding computer systems. The objective of IDS is to detect unauthorized use, misuse and abuse of computer systems. The intruders can either be system insiders or external intruders. Most of the IDS identify suspicious signatures based on known intrusions and probes [3]. Thus, limiting detection to only previously known intrusions, and failing to detect previously unknown intrusions. This failing is overcome by the use of AIS. AIS is based on the principle of HIS, which adaptively generates new immune cells that are capable of detecting previously unknown and rapidly evolving harmful antigens [4].

An IDS checks the connection records, traffic control packets for identifying the intrusion or attacks. The amount of records generated by a network is huge in quantity. Features are extracted from the records by the IDS and then classified to identify the record/connection as attack or normal traffic. To facilitate the machine learning methods used for classification, it is feasible to reduce the dimension of the feature. Feature reduction refers to mapping of data into lower dimension space. Feature extraction mainly involves feature selection, space dimensionality reduction. These techniques are used in pre-processing the data before used as inputs to machine learning and statistics tasks. Efficient feature extraction contributes to improved classification; lower pre-processing costs. This leads to improved overall performance of classifier based intrusion detection systems. Principal Component Analysis (PCA) is a technique for dimensionality reduction. It is a method of identifying data patterns and expressing it in a way to highlight both similarities and differences. In this paper, PCA is used for feature extraction.

II. Related Works

Hayoung et al., [5] suggested a SOM based real-time intrusion detection system that groups and visualizes similar data. The system labels the SOM produced map through feature correlation. Researchers experimented with the system using the 1999 data set of the KDD Cup. The system led to light misclassification rates and takes 0.5 seconds to discover whether behavior is normal or an attack. While unsupervised learning techniques are appropriate for anomalous behaviors, new attacks in a dynamic intrusion detection environment accommodate change in attack characteristics especially in MSN. SOM (Self-Organizing Map), a clustering algorithm is a data visualization technique that reduces data dimensions by using self-organized neural networks. SOM reduces dimensions by producing a map of 1 or 2 dimensions that plot data similarities and group similar data items. The system includes three steps as follows: Training, Labeling and Detection & Training. Training means creation of a map based on pre-processed/normalized data through SOM use. Labeling is classifying clusters from the trained map based on traffic feature correlations. Finally, Detection & Training means real-time intrusion detection and the continued training to adapt the system to new data. The system experiments yielded reasonable misclassification rates, and have the each attack’s characteristics whose unclassifiable features seem to have no relations among themselves. Feature correlation results are used in other intrusion detection systems with other technologies even when there is a new attack as time leads to adjustment of correlation information. The authors analyzed attacks with lack of clear characteristics like Smurf, extract features to reduce process overhead ending with the system being more accurate.

David Nguyen et al., [6] developed PCA architecture for outlier detection of high-speed network intrusion detection systems (NIDS). PCA is a common statistical method for use in multivariate optimization problems to reduce data dimensionality while retaining a large fraction of the characteristics of data. First, PCA projects the training set onto eigenspace vectors representing data mean. These eigenspace vectors then predict malicious connections in a workload with normal and attack behavior. Simulations revealed that architecture classifies attacks correctly and detection rates exceed 99%. False alarms rates low at 1.95%. For next generation NIDS, anomaly detection methods must meet the demands of Gigabit Ethernet. FPGAs handle both high throughput and adaptability to the dynamic nature of intrusion detection. The architecture was implemented - using hardware parallelism and extensive pipelining - on FPGAs to achieve Gigabit link speeds.

Stefan et al., [7] surveyed architecture and AI aspects in early warning and intrusion detection based on combined AI methods. They also addressed alarm assessment problems in intrusion detection and used plan reconstruction - based on organized procedural knowledge - containing adversary action descriptions.. Reconstructed plans correlate events and alarms from a SIEM and give security expert, explanations. It also aims to predict the next stage in multi-stage intrusion attacks on computer networks. Hence a proposal was made for probabilistic relational reasoning over time method based on hidden Markov models. Complementing anomaly-based IDS, early warning system based on heterogeneous methods of Artificial Intelligence (AI) was developed which supports a security officer in analyzing attacks and responding with counter measures. Consequently, the FIDeS project focused on assistance and not on mere intrusion detection. Different AI-based methods like declarative knowledge representation, the generation of explanations, and cognitive assistance are employed for this purpose. But integration with anomaly-based IDS is under study. The author planned to develop a system with machine-learning methods to improve detecting network attack quality and support users with enriched assistance in usage of SIEM offered event data. Hence the proposed system was divided into three core areas: Detection and attack explanation, attack prediction of attacks and user assistance to react on such detection. The method provides the ability to train a prediction for general attack patterns.

Bose et al., [8] focused on a new anomaly detection system for each network node containing detection subsystem for MAC, routing and application layers. Audit data from MAC level/Network level/Application level from Glomosim traces and are preprocessed differently for the detection subsystem of each layer. Normal transactions lead to selection of feature data sets for each layer. The Detection subsystem has normal profiles from training data set feature vectors. The work used Bayesian classification algorithm, Markov chain construction algorithm and association rule mining algorithm for anomaly detection in MAC, routing and application layers respectively for intrusion detection. Test data from network traffic is fed to detection subsystems. Any deviation from normal behavior is considered abnormal or an anomaly based on predefined thresholds. There are 3 types of intrusion detection and they include 1. Anomaly detection: Deviation from baseline profile of normal systems. 2. Misuse detection: On the basis of an intrusion process. 3. Specification-based detection: Defines set of constraints (correct operation of a program/protocol). GloMoSim 2.03 generates normal and abnormal data sets for anomaly detection systems. Java 1.5 and Active perl 5.8 implement an anomaly detection system. GloMoSim needs Microsoft VC++ 6.0 for run. Windows 2000 platform is used. Configuration settings simulating ad hoc network environment Intrusion results from detection subsystems of three layers are integrated and the final result is sent to global integration module. Intrusion results are received from neighbor nodes and are forwarded to the global integration module for a final decision.

Xiao et al., [9] presented methods to improve performance of IDS in two aspects: feature subset selection and parameter of SVM optimization. Ad hoc technology optimized feature subset for raw data and 10-fold cross validation is used to optimize SVM parameters for intrusion detection. There are many reasons to reduce features number to a minimum. Computational complexity is obvious. Though two features may carry good classification information when treated separately, there is little gain when combined together in a features vector, due to mutual correlation. A big advantage of handling features individually is computational simplicity. But they do not account for correlations between features. To deal with this, feature vectors utilized an “ad hoc” technique incorporating correlation information together with criteria readied for scalar features. Experiment data was prepared by the 1998 DARPA intrusion detection evaluation program in the MIT Lincoln Lab. The data set contains 24 attack types classified into 4 categories namely denial of service (DOS), remote to user (R2L), user to root (U2R) and probing. The main features in this paper were successful detection to achieve a high detection rate with sample for MIT lab, due to two reasons: first, some features might be redundant as information they have is contained in other features; secondly, extra features increases computation time, and impacts accuracy of IDS. Feature selection was built to improve classification by searching for features subset. This best classifies both training and testing data. The experiments results reveal that SVM with FS was not only superior to both famous data mining strategy and other intelligent paradigms.

In this paper, an intrusion detection system is proposed based on PCA and AIS. PCA is used for feature selection and AIS is used as classifier. The following section discusses the related works, materials and methods and the results.

III. Materials and Methods

A. Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is a technique for dimensionality reduction and multivariate analysis [10]. Its applications include data compression, image processing, visualization, exploratory data analysis, pattern recognition, and time series prediction. PCA popularity is derived from three properties. To begin with, it is an optimal linear scheme for compressing high dimensional vectors into lower dimensional vectors and later reconstructing the original set. Secondly, the model parameters are directly computed from data - by diagonalizing the sample covariance matrix. Finally, compression and decompression are easy to perform with the given model parameters - they need matrix multiplication alone. A multi-dimensional hyper-space is usually hard to visualize. The aim of unsupervised learning methods is reduced dimensionality, scoring observations on a composite index and clustering similar multivariate attribute observations. Multivariate attributes can be summarized by two or three variables which are graphically displayed with minimum information loss and are thus useful in knowledge discovery. As visualization of multi-dimensional space is difficult, PCA is used to reduce dimensionality of *d* multivariate attributes into two or three dimensions. PCA summarizes variations in correlated multivariate attributes to non-correlated components, each being of a particular linear combination of original variables. Thus extracted non-correlated components are known as Principal Components (PC) and they are estimated from the original variables eigenvectors. Hence PCA objective is achievement of parsimony and reduction in dimensionality through extraction of the smallest number components that lead to the most variation in original multivariate data. And this data should also be summarized with little information loss. In PCA, PC extractions can be made through original multivariate data set or by using a covariance matrix when the original data set is unavailable. In deriving PC, the correlation matrix instead of the covariance matrix might be used specially when differing dataset variables are measured with differing units or if differing variables have different variances. Use of a correlation matrix is equal to standardizing variables to zero mean and unit standard deviation.

The PCA model can be represented by:

$$u_{mx1} = W_{mxd} x_{dx1}$$

where *u*, an *m*-dimensional vector, is a projection of *x* - the original *d*-dimensional data vector (*m* << *d*).

B. *Artificial Immune Systems (AIS)*

Artificial Immune Systems (AIS) [11] is diverse areas of researches that attempts to bridge the divide between immunology and engineering and are developed through the application of techniques such as mathematical and computational modeling of immunology, abstraction from those models into algorithm (and system) design and implementation in the context of engineering. AIS have become known as an area of computer science and engineering that uses immune system metaphors for the creation of novel solutions to problems.

AIS is a model of the immune system that can be used by immunologists for explanation, experimentation and prediction activities that would be difficult or impossible in 'wet-lab' experiments. This is also known as 'computational immunology.' There is significant debate about the nature of the immunological mechanism that distinguishes between an organism's 'self' molecules and cells and an invading 'nonself' entity.

The obvious feature of the AIS is its ability to protect an organism from harmful agents known as pathogens, such as bacteria and virus. The concept is simple: Find the pathogen, identify it as harmful, and destroy it. The cell responsible for this is the lymphocyte. Assuming the pathogen has already been found, the distinguishing between harmful and harmless is the focus of our attention, and the destruction of harmful pathogens is replaced in an implementation by a context-appropriate response [12]. The objective of AIS in anomaly detection is to minimize damage while maximizing usability. But being completely usable, the system would have no protection, being completely safe the system would not be usable. Once again it is a matter of balancing requirements.

IV. RESULTS

The experiments were conducted using KDD 99 dataset on WEKA platform. A subset of 36496 instances was used with 18 attributes for the evaluation purpose. 66% of the dataset was used for training the classifier and the remaining for testing. Initial experiments were conducted without any dimension reduction of the feature set. Second set of experiments were conducted on a reduced dataset by applying PCA. Table 1 tabulates the training summary of Artificial Immune Recognition System without and with PCA and Table 2 and Figure 1 gives the summary of results.

Table 1: the training summary of Artificial Immune System without and with PCA

	AIS	AIS with PCA
Affinity Threshold	.0.227	0.058
Total training instances	36,496	36,496
Total memory cell replacements	36,049	35,884
Mean ARB clones per refinement iteration	51.313	51.817
Mean total resources per refinement iteration	126.285	126.81
Mean pool size per refinement iteration	69.617	70.307
Mean memory cell clones per antigen	19.606	19.979
Mean ARB refinement iterations per antigen	2	2
Mean ARB prunings per refinement iteration	53.616	54.307

Table 2: Summary of results

	AIS	AIS with PCA
Correctly Classified Instances	12149 (97.90 %)	12352 (99.54 %)
Incorrectly Classified Instances	260 (2.09 %)	57 (0.45 %)
Kappa statistic	0.6848	0.9029
Mean absolute error	0.0105	0.0023
Root mean squared error	0.1024	0.0479
Relative absolute error	44.53%	9.76%
Root relative squared error	93.72%	43.88%
Total Number of Instances	12409	12409

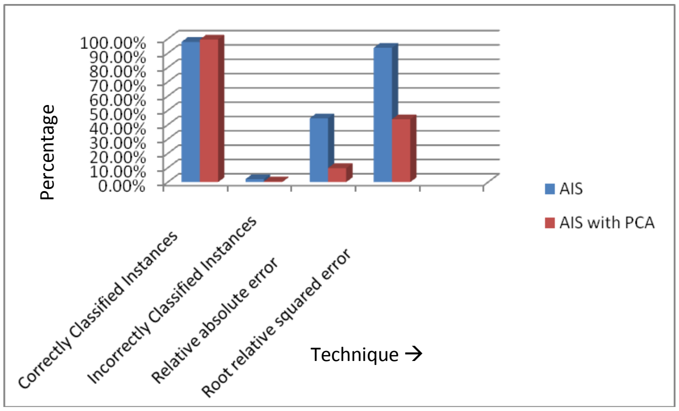

Fig. 1: Summary of results

Table 3: Detailed Accuracy by Class for proposed IDS with AIS and PCA

TP Rate	FP Rate	Precision	Recall	F-Mea	ROC Area	Class
0.998	0.103	0.997	0.998	0.998	0.947	normal.
0.603	0.002	0.677	0.603	0.638	0.801	teardrop.
0.987	0	0.987	0.987	0.987	0.993	satan.
1	0	0.963	1	0.981	1	nmap.
0.995	0.101	0.995	0.995	0.995	0.947	Weighted Avg

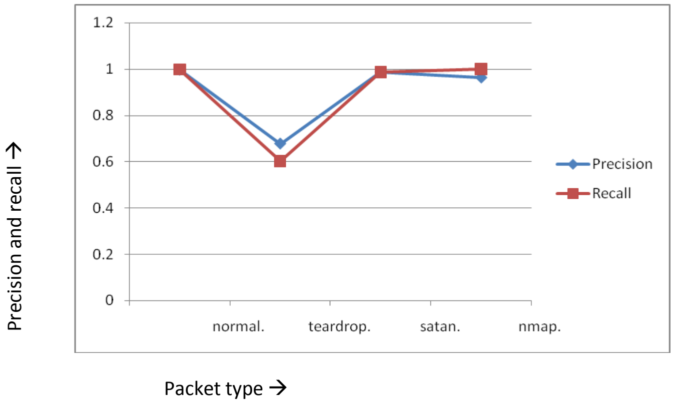

Fig. 2: Precision and Recall by Class for proposed IDS with AIS and PCA

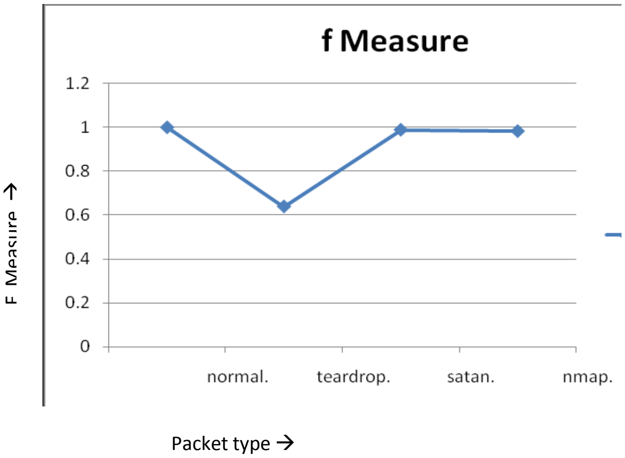

Fig. 3: f Measure by Class for proposed IDS with AIS and PCA

Table 4: Confusion Matrix

a	b	c	d	classified as
12082	21	2	3	a = normal.
29	44	0	0	b = teardrop.
2	0	148	0	c = satan.
0	0	0	78	d = nmap.

V. CONCLUSION

In this paper it was proposed to investigate the effectiveness of Artificial Immune System (AIS) as an classifier for Intrusion Detection System (IDS). Comparison was also done for the effectiveness of the classification accuracy after finding the eigen vectors of the attributes. Result shows an improvement in the classification accuracy.

REFERENCES

[1] Vera Marinova-Boncheva, (2007), “A Short Survey of Intrusion Detection Systems”, Problems of Engineering Cybernetics And Robotics, pp. 23–30.

[2] Paul Innella and Oba McMillan, (2010),”An Introduction to Intrusion Detection Systems”, Tetrad Digital Integrity, LLC.

[3] Kim J, Bentley P (1999),” The Artificial Immune Model for Network Intrusion Detection”, 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99).

[4] Kuby J (2002),” Immunology”, Fifth Edition by Richard A. Goldsby et al

[5] Hayoung Oh, Inshil Doh, Kijoon Chae,**(**2009),” Attack Classification Based On Data Mining Technique And Its Application For Reliable Medical Sensor Communication”, International Journal of Computer Science and Applications, Technomathematics Research Foundation, Vol. 6, No. 3, pp 20–32.

[6] David Nguyen, Abhishek Das, Gokhan Memik, and Alok Choudhary, (2006), “A Reconfigurable Architecture for Network Intrusion Detection using Principal Component Analysis”, Proceedings of the 2006 ACM/SIGDA 14th international symposium on Field programmable gate arrays Pages 235–235.

[7] Stefan Edelkamp , Carsten Elfersm, Mirko Horstmann ,Marcus-Sebastian Schr¨oder, Karsten Sohr and Thomas Wagner, (2009),” EarlyWarning and Intrusion Detection based on Combined AI Methods”, American Association for Artificial Intelligence

[8] S. Bose, S. Bharathimurugan and A. Kannan, (, 2007),” Multi-Layer Integrated Anomaly Intrusion Detection System for Mobile Adhoc Networks”, IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24. pp.360-365.

[9] Xiao Haijun, Peng Fang, Wang Ling, Li Hongwei, (2007), “Ad hoc-Based Feature Selection and Support Vector Machine Classifier for Intrusion Detection ”,Proceedings of 2007 IEEE International Conference on Grey Systems and Intelligent Services, pp. 1117–1121.

[10] Khaled Labib and V. Rao Vemuri,(2004),”An Application of Principal Component Analysis to the Detection and Visualization of Computer Network Attacks”, A version of this paper appeared in the proceedings of SAR 2004

[11] Simon M. Garrett, , (2007), “How Do We Evaluate Artificial ImmuneSystems?”,Evolutionary Computation 13(2):, 2005 , Massachusetts Institute of Technology,pp. 145-178.

[12] PC HabibAwan, PC Khurrum Abdullah, Capt. Shahid Abbas, Capt. Ali,(2008),”ImplementationOf Smart Antenna System Using Genetic Algorithm And Artificial Immune System” 17th International Conference on Microwaves, Radar and Wireless Communications, PP:1-4.