Anomaly-Based Intrusion Detection System using Supervised Learning Algorithm Artificial Neural Network and Ant Colony Optimization with Feature Selection

Annu Raj, Monika poriye

Abstract: **In the advent of the cyber world, all know that cyber security is randomly used research area for researchers to secure host, network, and data because of increasingly complex attacks. In the advent of anomaly-based intrusion detection system, various techniques are applied to detect intrusion on system or network. This approach attains an extreme detection rate and accuracy but there may be overhead acquired to build and training them. The objective of this paper is to detect the intrusion of a system by proposing a Data mining technique which is based on supervised learning algorithm for training dataset. Artificial neural network (ANN) and Ant Colony Optimization (ACO) with feature selection are the basics of the proposed scheme. ACO work on a population-based algorithm and is motivated by the pheromone trail laying behavior of real ants, in which NSL-KDD Cup99 Dataset is used. Empirical Results clearly explain that the proposed system can attain an overall detection rate of 88% and time complexity of 0.343 sec, which is satisfactory when compared to other anomaly-based schemes.**

Keywords: Ant colony Optimization, PSO, Detection Rate, False alarm, Data mining, KDD Cup99, Confusion matrix, information security, firewall security.

I. INTRODUCTION

In the era of digitization of data, security of the Network is the main objective because network services are enormously increasing day by day and they are easily targeted by attackers. These types of attackers are harm network as well as host machine [1]. From past decade intrusion attacks are increased, so recover from this problem there are different approaches like firewall security, encryption, control access, VPN(virtual private network)[2,3], and IDS/IPS are used. Security of network define level of protection and primary objective of security is to achieve these principle; Confidentiality, Availability, and Integrity of data [4]. So that cyber security is subsequently turn to main concern. Researchers create a method for securing the system from an external device, programs, and that user/ attacker who's only goal to destroy security services of the network.

IDS are mostly used as a tool for secure network from intrusion type attacks. The IDS decide that supervised network traffic or system movement is nasty /malicious and triggers an alarm [5].

IDS are a most convenient tool for protecting network and system from an intrusion attack. IDS are work on both Network as well as Host. Network-based IDS are normally monitoring activities of network and Host based IDS are used for detecting attacks that it observes individual machines.

IDS work on knowledge and behavior bases, on bases of these, two types of techniques are defined named signature-based detection and Anomaly-based detection [6].

Signature-based (misuse detection) uses previously preserved database of known attacks and analyze data. If patterns are matched, an attack is detected. The strength of misuse detection is low false alarm rate and weakness is, not detecting unknown new attacks and also a variant of known attack [7].

Anomaly-based (behavior detection) scheme are used to detect the behavior of network if it is according to previously defined behavior, then this will be approved else generates an event. The network administrator is specialized skilled or trained w.r.t. the accepted behavior of the network. This method is capable of detecting unknown/new attacks using the behavior detection of the network if it is according to the previously working of a network then normal otherwise an intrusion occurs. [8].

For achieving high accuracy of behavioral decision researchers used Hybrid detection approach because this approach based on signatures and anomaly and improve false positive rate which was low in anomaly-based IDS. The main objective of the hybrid approach is to improve false alarms. Hybrid detection gives better performance in term of false positive rate and accuracy.

In this paper, supervised learning is used for detecting the behavior of network which is a Data mining technique. Supervised learning is used for training every data with reference to the targeted output, and after enough training, this will be capable to present a target for new inputs. The learning algorithms have various algorithms for individual input. Some of techniques are defined in Fig1.

Revised Manuscript Received on February 05, 2020

Miss. Annu Raj, Assistant professor, Vaish College of Engineering, Rohtak.

Mrs Monika Poriye, Assistant Professor, Department of Computer Science and Applications, Kurukshetra University Kurukshetra

Here, ANN is used for making efficient result for the fast training of dataset and detects dangerous attacks. The attack may be smurf (a Trojan attack), satan (Ransomware type attack) [9], Dos, and probe etc. Artificial neural networks learn actions and make a judgment by commenting on that action has ability for parallel processing. So in the proposed system, ANN is used with ACO to give fast processing and improve detection rate.

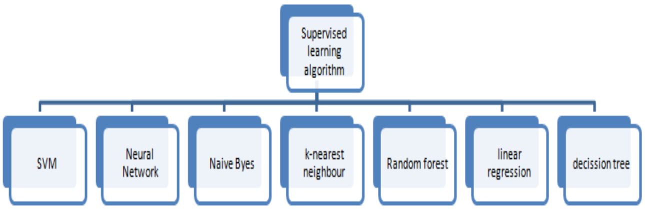


Fig1. Supervised Learning Algorithm [10]

ACO stands for Ant Colony Optimization which is a population-based approach for solving difficult combination problems. ACO working is inspired by the inbuilt behavior of ant for finding smallest path between food and their nest, or search strategies of ant.

II. RELEATED WORK

The author proposed [11] an effective scheme based on supervised learning algorithms that are used for comparison of Anomaly-based IDS using ANN and SVM with all dataset features. Using KDD Cup 99 data set for finding accuracy preprocessing applied to filtering and normalized attribute, which are DOS, U2R, R2L, and Probe. Support Vector Machine is not performing better than the Artificial neural network. ANN contains high accuracy and detection rate in all categories where author proved that NN has high accuracy for attack detection than SVM. Another machine learning technique is used to diminish huge number of a false alert. The paper [12] analyzes the supervised and unsupervised mechanism for handling the issue of anomaly detection. Supervised algorithms are KNN, NN, BN, BT, and SVM. Unsupervised algorithms are Clustering technique (SOM, K-Means, Fuzzy C-Means etc.), and OCSVM (One-class SVM), in which unsupervised algorithm K-Means, SOM and One-class SVM result in superior performance over another technique while they contradict in their capability to exposing all attacks.

The author reviewed to update previous anomaly-based IDS which are used rule based system those have some limitation to detect novel intrusion. So author proposed [8] new approach called Random forest (RF) using signature, behaviour, and hybrid- network IDSs. Data mining technique is used in Random forest which constructs pattern repeatedly for detecting intrusion by matching patterns with network activity. After building patterns anomaly detection uses outlier detecting algorithm for detect intrusion on network. Hybrid network intrusion detection system uses property of both misuses as well as anomaly detection. This approach of IDS improves the detection work. Using unsupervised anomaly detection technique this gains high rate detection and low false positive rate so we can say that overall performance for detecting anomalies was increased by hybrid approach.

Author Introducing a procedure for identifying and classifying anomaly using an artificial neural network (ANN) and evaluate data collected through Netflow protocol. This research work introduced using Multilayer perception trained with back propagation algorithm. Author experiment with dataset gathers from real ISP monitoring system and dataset altered imitation in existence of anomalies. Netflow record is altered to hold known patterns of different network attack, that assess practical experiment of approach with discrete anomalies and iteration sizes [13].

Author developed a [5] Fast learning network (FLN) model located on Particle swarm optimization (PSO) which is compared against meta-heuristic algorithm for training of classifier, FLN and ELM (Extreme Learning Machine). The PSO-FLN provides testing accuracy in form of output for learning and increases all models accuracy with increase in hidden neurons numbering. In this model there is problem arise from restricted quantity of training data results in less accuracy for certain number of class.

The author present that for detecting intrusion from system many techniques are invented, By using these techniques high detection rate and low false alarm rate are attained.IDS has variant signature-based Detection(SBD) and anomaly-based detection(ABD) and defines various anomaly detection techniques. Some anomaly detection techniques are Statistical based (Operational, Multivariate, Statistical moments, Time series, Univariate, Markov Process/Marker), Cognition based (Finite state machine, Description script, Expert system), and Machine learning (Bayesian Networks, Generic algorithms, Neural network, Fuzzy Logic, Outlier detection) etc. It is harder to compare advantages and disadvantages. This paper discusses detailed review and recognition of the deficiency of surveyed work [6].

Naïve Bayes algorithm is heavily simplified Bayesian probability model which consider end result probability and gives various linked evidence variables. The author build pattern of network services and detect attacks in a dataset using naïve Bayes algorithm, which as compared to NN with high detection rate, less time, low cost and generate more false positive. This algorithm supposes that there is totally independence between information nodes of two layers restricted network. This is disadvantages of naïve bays algorithm [14].

Author state that the growing of internet access increases the occurrence of cyber attacks. So tackle from these attacks high level of skills must be required to identify and resolve intrusion. If these intrusions can be identified prior then system can be protected from heavily type of losses. This paper discuss about the SVM classifier which classifies the data. SVM technique is mostly used data mining technique for classification. Intrusion detection system is usually used for preserving the "integrity of data, confidentiality and system availability from attacks". KDD Cup dataset is used to calculate the values of parameters which are used for finding performance evaluation.

"Validation Accuracy is equal to the number of samples recognize correctly and Classification Accuracy is equal to the number of total samples classified accurately". Only

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

one minimum value is required for training the data and for classifying huge amount of data. Therefore in future Support Vector Machine in grid environment can be used in new domain [15].

III. PROPOSED WORK

Methodology used:

System requirement:

For the proposed scheme 64-bit Operating system, 4 GB RAM, Intel corei5-3230M, 2.60 Ghz CPU, and Matlab software licensed are required.

MATLAB:

Initially Matlab is developed by Mathworks in 1984 and designed by Cleve Moler. This is multi-paradigm mathematical computing environment. Matlab is analyzing data, matrix manipulation, plotting of graph, develop an algorithm, create the mathematical model, and interfacing with another language with programs written in another language like C, C++, C#, Java, FORTRAN, and Python.

a. KDD Cup 99 Data set Reading and labeling:

From 1999, KDD CUP 99 is (mostly) used dataset for evaluation of the system. Two important issues are found by using statistical analysis behavior on a dataset that extremely affects the system performance and unfortunate estimate of result for anomaly detection approaches [16].

To recover from this problem a new data set is proposed named NSL-KDD. The modification in NSL-KDD data set is classified in train and test data set and also correcting the labeling. Attack defined in NSL-KDD dataset are normal, DOS (Denial of service), U2R (User to Root), R2L (Remote to Local), Probing attack. Researchers found some difficulty in using whole data set for training so that they take some relevant features (taking 10% of whole data) attribute for training [16,17].

a. Data Set Pre-Processing:

In preprocessing of dataset, cleaning and transformation are performed. Cleaning process means removing the redundant labels and filling missing value in the dataset. Transformation means translate full data set into the desired form (it means convert numeric value to the string type data).

b. Feature Extraction:

Feature Extraction is performed after labeling of data set that will eliminate extra dimension of big data set which have more features/attribute and are irrelevant. Dataset has duplicate data so it needs a transformation to decrease redundant feature from a dataset. The objective of feature extraction is to reduce dimension from a big dataset and improve accuracy by removing inappropriate data [18].

c. **Feature Selection with Ant Colony Optimization:**

In the proposed model of artificial neural network with Ant colony optimization performed a number of steps to classify KDD CUP 99 Data set into two categories i.e normal or attack. Generally, coming input from any source to the system is either attack (abnormal behavior or malicious activity) or normal (normal behavior). Thus, the proposed model is focusing on abnormal behavior and performed this model using following steps:

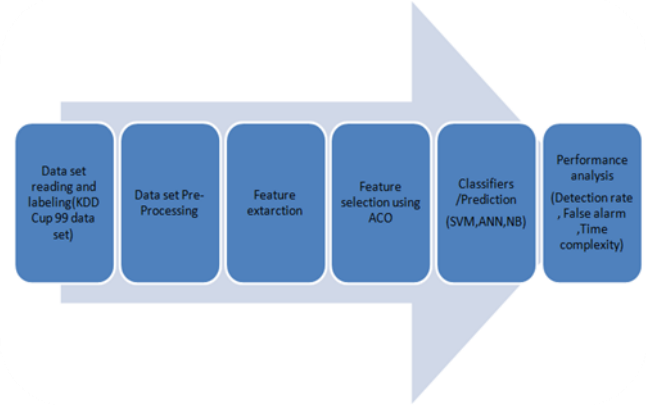

Data set reading and labeling(KDD Cup 99 data set)
Data set Pre-Processing
Feature extarction
Feature selection using ACO
Classifiers /Prediction (SVM,ANN,NB)
Performance analysis (Detection rate , False alarm ,Time complexity)

Fig2. Proposed work model

Feature selection is used to improve the overall classification accuracy by selecting main input training feature and eliminating unrelated input training. Here feature selection is used with ACO to improve accuracy and better results [19]. Feature selection is calculated by using Information gain in which I(S) stand for expected information and S used for a total count.

This will be calculated by using Eq 1

Information gain (G)= I(S)- $\sum_{j=1}^{v} \frac{|Sv|}{|S|} I(Sv)$ (1)

Here, $\sum_{j=1}^{v} \frac{|Sv|}{|S|} I(Sv)$ is the formula for Entropy (E (A)).

Ant Colony Optimization:

Ant colony optimization (ACO) is initially invented in 1992 by Colorni, Dorigo, and Maniezzo. ACO is a common search technique which is used to solve difficult conditional problems [20]. This is motivated by the pheromone track laying activities of real ants. Ant mostly walks arbitrarily through the path until they find the shortest path to food and come to nest. The behavior of ant colony is depending on autocatalysis which acquires positive feedback that will be used by ants to locate the shortest trail between nest and food. So choosing path probability is depend on pheromone amount at that path and discharge pheromone is communication medium between ant colonies [21].

Initially, Aim of the algorithm is a search for an optimal path in a graph, which originates from behavior of ants in search of a path from their colony and a source of food. The original data has since diversified to solve wider class of numerical problems. The main features are a high-precision solution, fast search speed, convergence to global optimum and greedy heuristic search [22].

Ant selection probability to a path is defined by objective function as follows:

$$p1 = \frac{(m1+k)^{h}}{(m1+k)^{h}+(m2+k)^{h}}) \qquad (1)$$

In Eq (1) p1 is for probability and m1 and m2 are a moment of time .where parameter k and h are fitted to the experiment. After each iteration value of pheromone are updated by all m ants those construct results in iteration itself. The pheromone is updated which is connected to edge joining points i and j as follows:

$$\tau_{ij} \leftarrow (1-\rho).\tau_{ij} + \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \qquad (2)$$

```
Pseudo Code:
Step1. Initialize the parameters, pheromone trail and set an ant on random location.
Step2.  Identify all the link and limiting criteria.
Step3. Generation of Artificial ant Agent and evaluate finest achievable solution form complete solution space take place using
Step4. Update pheromone trail using Local updating rule (end of each movement).
Step5. If all ants compute solution then terminate condition and go to next step
else, repeat from Steps3.
Step6. Compute length of optimal path and update only pheromone on the optimal path by using Global
 updating rule.
Step7.  If not satisfy then repeat iteration from step2.
else, optimal solution found that contains the maximum pheromone.
```

In Eq (2) ρ stands for evaporation rate, m for a number of ants, laid pheromone on (i,j) by kth ant. Pheromone is updated after next iteration t+1.

$$\tau(t+1) = (1-\rho)\,\tau_{ij}(t) + \Delta\tau_{ij}(t) \qquad (3)$$

$$\Delta\tau_{ij}(t) = \textstyle\sum_{h=1}^{m} \Delta\tau_{ij}^{k}\,(t) \qquad (4)$$

Eq (3, 4) shows that remaining pheromone is 1-ρ, m signify no of ant $\Delta\tau_{ij}^{k}$ is represent pheromone amount remaining on a path for that iteration k. Local and global updating rules decrease pheromone level lightly.

Particle Swarm Optimization:

Particle Swarm Optimization (PSO) belongs to swam intelligence and it was introduced in 1995 by Dr. Russell C, Kennedy & Eberhart [23]. PSO is parallel evolutionary computation technique and that is inspired by the social behavior of bird's flocking and fish schooling. It is simple to implement, scalable, robust, and quick in finding an approximately optimal solution and flexibility [24]. A particle moves towards using previous best position and global best position. Each iteration velocity is change by using current velocity of particle. After that, new velocity is used to calculate the position of the particle. The particle is performed this in multidimensional space which has some velocity and position.

Velocity update:

$$V(t+1) = \alpha Vi + c1 * rand * (pbest(t) - xi(t)) + c2 * rand * (gbest(t)-xi(t)) \qquad (5)$$

Where rand are used for random number, c1 and c2 are positive constant number. Eq (5) calculate the velocity changed after time (t+1),

Position Update:

$$Xi(t+1)=Xi(t)+Vi(t+1) \qquad (6)$$

Eq (6) determine position changed after velocity V(t+1).

IV. CLASSIFIER/ PREDECTION

There are various supervised learning algorithm are used to classify the problem. Some of them are following:

- **Artificial neural network:**

Proposed Artificial Neural Networks are work related to the behavior of human brain activities. Basically, the neural structure of intelligent and alive organisms able of obtain knowledge and experience above time is follow, which makes ANN technique totally diverse from digital computing and has a capability of manage their personal structure (called neurons) to deal with some precise computational activities. This is Information specific model which is inspired by biological neuron works such as brain, process information [25]. In which to perform pattern recognition network trained in a specific way that lead to exact output with reference to input. The

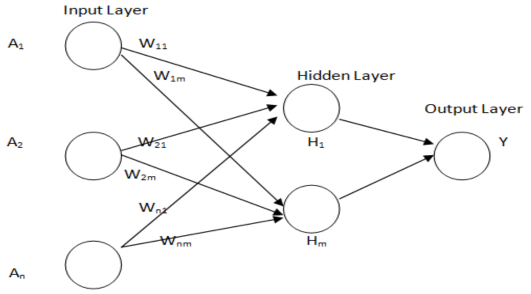


Fig3. Layered architecture of Artificial Neural Network

ANN remains constantly under adjustment through the comparison between the output and the target, until the network output is compatible with the target and the neurons have acquired the knowledge of the parameters to that specific application [26].

It is a group of an interconnected node like input layer, Hidden layer, and the Output layer. Hidden layer contain weight and process data and values are frequently adjusted during training of NN until reached to desired output.

- **Support Vector Machine:**

Support vector machine is most popular supervised learning data mining classification algorithm but it uses long training time. It is also previously applied on various real world applications like pattern recognition and hand-writing recognition etc and many more [19]. In SVM for training the data set, takes more time if dataset are too long for that there are to improve performance either user use random selection and approximation of trivial classifier. A new method is proposed to enhancing SVM training process use SVM with Clustering analysis [27].

The classification of SVM is established on the idea of decision boundaries and these decision boundaries split a set of example between two groups having diverse class values. In order to get result for recognizing patterns from training data, each instance belongs to one of two classes. This kind of binary classifier inspire researcher to apply this technique in to detecting attacks, classification in single class (normal and attacks).

In Fig4 one hyper- planes are created which classify the data and margin/separation between two classes. Here, Z1 separate two classes with maximum margin. So by using SVM detected attack is classified into categories normal and attack.

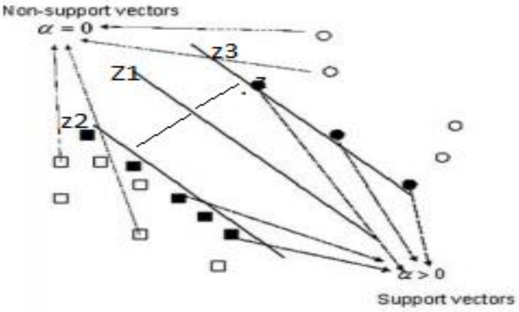


Fig4. Support Vector Machine [27]

SVM can perform through Linear Classification (Originated in 1963) and Non-Linear Classification (Originated in 1992) using kernel trick. Non-Linear Classification performs through implicitly mapping their input into high-dimensional feature space. If the data is not labeled, then SVM can be used as clustering technique. Some of Real world's applications are face detection, classification of image, text and hypertext categorization etc. After training data it gives best accuracy and removes over a fitting problem.

- **Naïve Bayes:**

Naïve Bayes is classification model which is based on a Bayesian probabilistic model of the Thomas Bayes [28].This will work on an independent assumption so probability of one does not affect others probability [29].This model work on posterior, prior, likelihood and evidence.

likelikhood prior probability

posterior probability

$$P(t \mid y) = \frac{P(y \mid t)P(t)}{P(y)}$$

evidence

$$P(t \mid y) = P(y_1|t) * P(y_2|t) * - - - * P(y_n|t) * P(t) \qquad (7)$$

Naïve Bayes classifier.

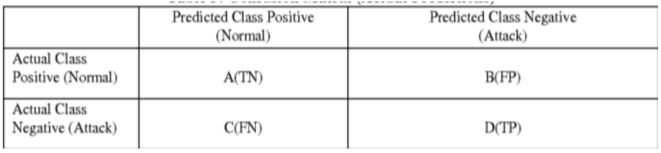
Here, t is defined as target class which is an attack or normal and y is an attribute represents ($y=y_1+y_2+y_3+$-------$+y_n$) n features. Prior probability is defined by the previous knowledge that is an attack or normal. Where likelihood also termed as posterior probability, classes are described after applying this method. The evidence is a probability of emerging attacks categories in KDD dataset. In the end, Higher probability shows that input dataset either attack or normal. A major drawback of naïve Bayes is independent assumption, thus it is not worth for real-world problem. Some of their applications are Sentiment Analysis, Document Categorization, Email spam filtering. The benefits of Naïve bayes classifier are, it works for both discrete and continuous attribute on same data set at the same time with accurate prediction on test data as well as work on multiple dataset [30].

V. PERFORMANCE ANALYSIS

The performance of the proposed model ACO with ANN is described by the Confusion Matrix.

Confusion Matrix:

Confusion Matrix represents the accuracy of used classifier for proposed scheme. Its right classifications as 'true positives' or 'true negatives', and wrong classifications as 'false positives' or 'false negatives'. Also have possibility to derive the accuracy, detection rate, false alarm, time complexity and others factors. Misclassified data is represented by off-diagonal elements in confusion matrix. In which every row of matrix represent actual class and every column represent instance of predicted class [31].



	Predicted Class Positive (Normal)	Predicted Class Negative (Attack)
Actual Class Positive (Normal)	A(TN)	B(FP)
Actual Class Negative (Attack)	C(FN)	D(TP)

Fig5. Confusion Matrix

Detection rate: Detection rate are also known as sensitivity, it define test capability to detect correctly attacks.

Detection rate= TP/(TP+FN)*100

Accuracy: This is the quality or state of being correct or exact.

Accuracy=TP+TN/TP+TN+FP+FN

False Alarm rate: False alarm rate are the probability defined null hypothesis which is the falsely rejecting from a particular test.

False Alarm Rate=FP/(FP+TN)*100

Time complexity: This will be signifies by time taken to provide results. It means on what iteration result will be given by classifier.

Performance of the proposed model is also evaluated by other parameters likes accuracy, F-Measure, precision, and recall etc.

VI. EXPERIMENT/RESULTS

The proposed method is applied to the single class dataset by using feature selection with Ant Colony Optimization (ACO) on different combination of the classifier. The previous work on PSO-FLN [5] gives better result in testing accuracy but it may take more time and have high False alarm rate.

Table 1 clear that the combination of ACO and ANN give better result in every field has higher detection rate (Accuracy) with low False Alarm Rate and with decreased Time complexity. PSO-ANN results are also better than others but this will not compete ACO-ANN results.

Classifier/ Approach	DetectionRate %	FalseAlarmRate %	TimeComplexity (Sec)
ACO+SVM	87.8152	12.1848	4.735
PSO+SVM	83.8604	16.1396	4.213
ACO+NB	84.5419	15.7784	1.254
PSO+NB	84.2216	15.7784	1.279
ACO+ANN	88.2987	11.7013	0.343
PSO+ANN	82.1422	17.8578	0.409

Table 1.Results after apply ACO and PSO

Results of the proposed approach are defined in graphs form with reference to detection rate, false alarm and time complexity.

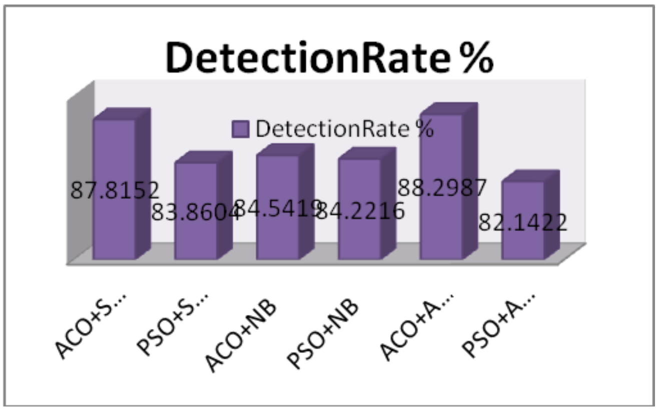


Fig 6 Detection Rate

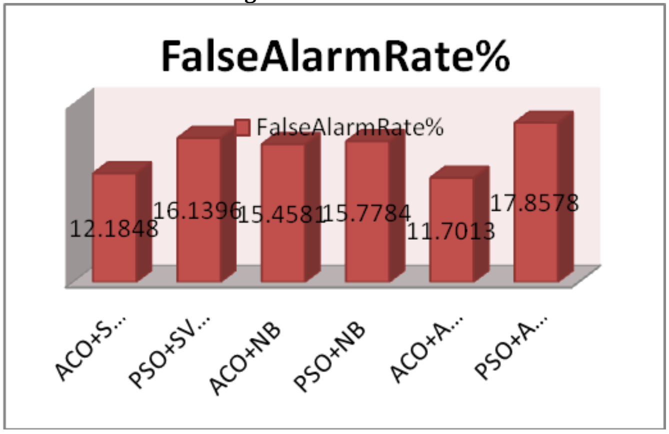


Fig 7 False Alarm Rate

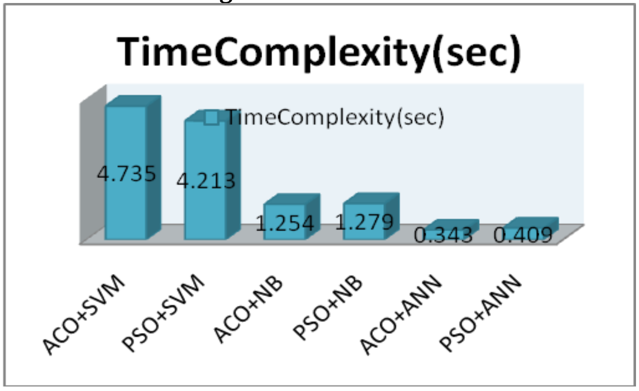


Fig 8 Time Complexity

In which, in Fig 6 proposed scheme achieve improved detection rate 88.30%, Fig 7 define decreases in false alarm rate 11.70% and in Fig 8 reduce time complexity up to 0.34 sec. Overall performance has been improved with this experiment.

Proposed model verified that Ant Colony optimization gives better result with an artificial neural network. Thus, the model might be used for fast training, testing of dataset and also for detection of malicious activity.

VII. CONCLUSION & FUTURE SCOPE

In this Paper, a new framework is proposed based on supervised learning anomaly detection scheme using ACO-ANN, which improves performance and securing network from attacks (Trojan, Ransomware etc.). In which performing different combination with ACO and PSO gives improved result when this will be used with ANN, NB, and SVM classifiers. The main idea of purposed model is to improve detection rate, false alarm and time complexity during training and testing of the system which was attained successfully. ACO-SVM gives a better result for detection rate and false alarm rate among all except ACO-ANN but this takes more time to do this. Therefore combining ACO-ANN improves results for detecting destructive malware in anomaly-based intrusion detecting system.

The future work focuses on improving all other factors of performance analysis by using another algorithm of a neural network with proposed approach for anomaly detection up to (99.9%) and this approach also applicable with another type of dataset which has dangerous malware like advanced ransomware and Trojan attack. By using Deep learning approach the performance of IDS can be improved.

REFERENCES

1. Matthew Bailey, Connor Collins, Matthew Sinda and Gongzhu Hu, “Intrusion Detection Using Clustering of Netwrok Traffic Flows”, IEEE, 978-1-5090-5504-3/17/2017.
2. Monika and Swati Kapoor, “Mitigating DoS Attack in VPN”, International Journal of Computer Trends and Technology (IJCTT), volume 4, Issue 5, pp 1191-1195, 2013.
3. Monika and Swati Kapoor, “Virtual Private Network-A Review”, National conference on Advanced Computing Technologies, Vol 1, March 2013.
4. Rashmi Ravindra Chaudhari and Sonal Pramod Patil, “Intrusion Detection System: Classification, Techniques And Datasets To Implement”, International Research Journal of Engineering and Technology, e-ISSN: 2395-0056, p-ISSN: 2395-0072, Vol. 04, Issue. 02, Feb 2017.
5. Mohammed Hasana Ali, Bahaa Abbas Dawood AL Mohammed, Madya Alyani Binti Ismail, Mohamad Fadli Zolkipli, “A new intrusion detection system based on Fast Learning Network and Particle swarm optimization”, Vol. XX, ISSN: 2169-3536, DOI:10.1109, Access.2018.2820092, IEEE, 2017.
6. V. Jyothsna and V.V. Rama Prasad, “A Review of Anomaly based Intrusion detection System”,International Journal of Computer Application, ISSN:0975-8887), Volume 28-No.7,September 2011.
7. J. Rene Beulah AND D. Shalini Punithavathani, “Applying Outlier Detection Techniques in Anomaly-based Network Intrusion Systems – A Theoretical Analysis”, International Journal of Computer Applications on International Seminar on Computer Vision, ISSN: 0975 – 8887, 2013.
8. Jiong Zhang And Mohammad Zulkernine and Anwar Haque, “Random-Forests-Based Network Intrusion Detection Systems”, ISSN: 1094-6977, Vol.38, No.5, IEEE, Sepetember2008.
9. Annu, Monika Poriye, and Vinod kumar, “Ransomware: Detection and Prevention”, International Journal of Computer Science of Engineering, Issue 6, Vol 5, pp 900-905, May 2018.
10. Panos Louridas and Christof Ebert, “Machine Learning”, Published By The Ieee Computer Society, 0740-7459/16, pp 110-115, IEEE 2016.
11. Adtiya Nur Cahyo ,Risanuri Hidayat, and Dani Adhipta, “Performance Comparison of Intrusion Detection System based Anomaly Detection using Artificial Neural Network and Support vector Machine ”, Advances of science and technology for society,978-0-7354-1413-6,doi-10.10631/1.4958506,2016.
12. Salima Omar, Asri Ngadi, and Hamid H. Jebur , “Machine Learning Techniques for Anomaly detection: An Overview”, Internation Journal of Computer Application,ISSN: 0975-8887, Volume 79-No.2 October, 2013.
13. Sergay Andropov, Alexei Guirik, Mikhail Budko and Marina Budko, “Network Anomaly Detection using Artificial Neural Network ”,Open Innovation Association(FRUCT) 20th Conference,2017,ISSN NO:2305-7254,IEEE 2017.
14. Mrutyunjaya Panda and Manas Ranjan Patra, “Network Intrusion Detection Using Naïve Bayes ”, International Journal of Computer science and Network Security, Vol. 7, No. 12, December 2007.
15. Manjiri V. Kotpalliwar and Rakhi Wajgi, “Classification of Attacks Using Support Vector Machine (SVM) on KDDCUP'99 IDS Database”, Fifth International Conference on Communication Systems and Network Technologies, 978-1-4799-1797-6, pp: 987-990, April 2015.
16. Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A.

Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set", IEEE, 978-1-4244-3764-1/09/2009.

17. "Nsl-kdd data set for network-based intrusion detection systems." http://www.unb.ca/cic/datasets/nsl.html, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed on 10 May, 2019).
18. O. Isaiah Aladesote ,Agbelusi Olutola, and Olasehinde Olayemi, "Feature or Attribute Extraction for Intrusion Detection System using Gain Ratio and Principal Component Analysis (PCA)", Communications on Applied Electronics (CAE) – ISSN : 2394-4714, Volume 4– No.3, January 2016.
19. Muhammad shakilpervez and Dewan Md. Farid, "Feature Selection and Intrusion Classification in NSL-KDD Cup 99 Dataset Employing SVMs", IEEE, 978-1-4799-6399-7/14, 2014.
20. Namita Shrivastava and Vineet Richariya, "Ant Colony Optimization with Classification Algorithms used Intrusion detection", International journal of computational Engineering & Management, Vol. 15, Issue. 1, ISSN: 2230-7893, January, 2012.
21. Yang Xianfeng and Li HongTao, "Load Balancing of Virtual Machines in Cloud Computing Environment Using Improved Ant Colony Optimization", International journal of Grid Distribution computing, Vol. 8, No. 6, pp. 19-30, ISSN: 2005-4262, IJGDC, 2015.
22. Wenming Huang, Zhenrong Deng, Peizhi Wen. "Trust-Based Ant Colony Optimization for Grid Resource Scheduling", 2009 Third International Conference on Genetic and Evolutionary Computing, 2009
23. Harshit Saxena, Dr. Vineet Richariya, "Intrusion Detection System using K- means, PSO with SVM Classifier: A Survey", International Journal of Emerging Technology and Advanced Engineering (IJETAE), Volume 4, Issue 2, February 2014.
24. Seyed Mojtaba Hosseini Bamakan., Behnam Amiric, Mahboubeh Mirzabagheri, and Yong Shi, "A New Intrusion Detection Approach using PSO based Multiple Criteria Linear Programming", Information Technology and Quantitative Management (ITQM) published by Elsevier , doi: 10.1016/j.procs.2015.07.040, 2015.
25. Devikrishna K S and Ramakrishna B, "An Artificial Neural Network based Intrusion Detection System and Classification of Attacks", International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 3, Issue 4, pp. 1959-1964, Aug 2013.
26. L.P. Dias, J.J.F. Cerqueira, K.D.R. Assis and R.C. Almeida Jr, "Using Artificial Neural Network in Intrusion Detection System to Computer Network", IEEE, 978-1-5386-3007-5/17, 2017.
27. Latifur Khan · Mamoun Awad · Bhavani Thuraisingham, "A new intrusion detection system using support vector machines and hierarchical clustering", The VLDB Journal, DOI 10.1007/s00778-006-0002-5, 2007.
28. Shyara Taruna R. and Mrs. Saroj Hiranwal, "Enhanced Naïve Bayes Algorithm for Intrusion Detection in Data Mining", International Journal of Computer Science and Information Technologies, Vol. 4 (6), ISSN: 0975-9646, IJCSIT, 2013.
29. Dr. Saurabh Mukherjeea , Neelam Sharmaa , "Intrusion Detection using Naive Bayes Classifier with Feature Reduction", doi: 10.1016, ISSN: 2212-0173, Elsevier, 2012.
30. Sona Taheri and Musa Mammadov, "Learning the Naive Bayes Classifier with optimization models", International Journal of Applied Mathematics and Computer Science, 2013, Vol. 23, No. 4, 787–79, DOI: 10.2478/amcs-2013-0059.
31. A. K. Santra and C. Josephine Christy, "Genetic Algorithm and Confusion Matrix for Document Clustering", International Journal of Computer Science(IJCS) Issues, Vol. 9, Issue 1, No 2, January 2012 ISSN : 1694-0814.

AUTHORS PROFILE

Miss. Annu Raj currently working as Assistant professor in Vaish college of engineering, Rohtak. I pursed B.tech form MDU University of Rohtak, in 2015, Diploma in Computer Scinece and Engineering form HSBTE, Panchkula, in 2012 and currently I did M.tech from Kurukshetra University Kurukshetra Department of Computer Science and Applications in 2018. My research work under M.tech is focuses on Ransomware detection using Intrusion detection system.

Mrs Monika Poriye is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science and Applications, Kurukshetra University Kurukshetra. Her main research work focuses on Security in wireless Sensor Netwrok during Ph.D..