ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 317-323 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

A Hybrid Approach for Intrusion Detection using Integrated K-Means based ANN with PSO Optimization

Jesuretnam Josemila Baby*, James Rose Jeba

Noorul Islam Centre for Higher Education, Department of Computer Applications, Noorul Islam University, Kumaracoil, 629180, India

ARTICLE INFO

Article history:
Received: 04 February, 2020
Accepted: 24 May, 2020
Online: 29 May, 2020

Keywords:
Particle Swarm Optimization
Intrusion Detection System
Artificial Neural Networks

ABSTRACT

Many advances in computer systems and IT infrastructures increases the risks associated with the use of these technologies. Specifically, intrusion into computer systems by unauthorized users is a growing problem and it is very challenging to detect. Intrusion detection technologies are therefore becoming extremely important to improve the overall security of computer systems. In the past decades, most of the intrusion detection systems designed suffer from the problem of high false negative and low efficiency rate. A powerful intrusion detection system (IDS) should be implemented to solve these issues and it is necessary to collect, reduce and analysis the data automatically. The integration of machine learning and artificial intelligence techniques serves this purpose in this paper. A use of particle swarm optimization (PSO) selects the optimal number of clusters and the integration of k-means based artificial neural network (ANN) achieves maximum efficiency when the number of clusters selected optimally. The proposed IDS are t bested with NSL-KD dataset and the experiment result shows the significance of the proposed IDS.

1. Introduction

Due to the advancement of computer and communication technology, the reliance on Internet and worldwide connectivity, damages caused by unexpected intrusions. These crimes related to computer systems have been increased rapidly; a computer system should provide confidentiality, integrity and availability against denial of service; therefore, it is very important that the security mechanisms of systems be designed to prevent unauthorized access to system resources and data [1]. Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks by isolating these networks using the rules and policies determined for them [2]. However, it is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not [3]. This is the situation where intrusions detection systems (IDSs) are in charge.

Intrusion detection Systems (IDSs) is a software or device that helps to resist network attacks [4]. The goal of IDS is to have defense wall, which does not allow such types of attacks [5]. It detects unauthorized activities of a computer system or a network. IDS are an active and secure technology there are two categories of intrusion detection system [6].Anomaly detection system creates a database of normal behavior and any deviations from the normal behavior are occurred an alert is triggered regarding the occurrence of intrusions [7]. Misuse Detection system stores the Predefined attack patterns in the database if a similar data and if similar situations occur it is classified as attack. Based on the source of data the intrusion detection system is classified to Host based IDS and Network based IDS [8]. In network-based IDS the individual packet flowing through the network are analyzed [9]. The host-based IDS analyzes the activities on the single computer or host [10]. The main disadvantage of the misuse detection (signature detection) method is that it cannot detect novel attacks and variation of known attacks [11]. To avoid these drawbacks, we proposed anomaly-based detection methods.

Most unsupervised anomaly detection methods are established on two basic assumptions about data [12]. First, the number of normal instances vastly outnumbers that of anomalies. Second, data instances of the same classification (type of attack or normal) should be close to each other in the feature space under some reasonable metrics, and instances of different classifications are far apart [13].Data mining technique is used to find the interesting rules from a large database depending

* Jesuretnam Josemila Baby, Email: josemilakissinger@gmail.com

upon the user defined support and confidence [14]. It will be useful for the decision maker to differentiate between data as useful or irrelevant [15]. Clustering is the unsupervised classification of input items into groups (clusters) without any prior knowledge [16].

Although many kinds of clustering methods, such as Fuzzy C-Means (FCM), K-means, are widely used in intrusion detection, few clustering algorithms guarantee a global optimal solution [17]. Based on this intention we developed a new anomaly intrusion detection mechanism employed with multi-dimensional hierarchical k-means algorithm in this research work in order to overcome all the above issues [18].To integrate K-means and Artificial Neural Network (ANN) technique with optimization to propose an efficient IDS with High True Positive Rate(TPR) and Low False Negative Rate(FNR) [19].

The organization of the paper is as follows: In Section 2, discuss about the related work with emphasis on various methods and frameworks used for intrusion detection. Section 3 covers the Integrated K-Means based ANN with PSO Optimization algorithm. Section 4 presents the experimental results and comparison of the proposed method with other approaches. It is observed that the proposed system. Section 5 gives some conclusions.

2. Related Work

Sharma, Ruby, and Sandeep Chaurasia (2018) [20] proposed an Intrusion Detection System based on the density maximization-based fuzzy c-means clustering (DM-FCC). In that approach, cluster efficiency was improved through a membership matrix generation (MMG) algorithm. Dissimilarity Distance Function (DDF) has been used to compute the distance metric while creating a cluster in proposing IDS. The proposed enhanced fuzzy c-means algorithm has been tested up on ADFA Dataset and the model performs highly appreciable in terms of accuracy, precision, detection rates, and false alarms.

Chung, Yuk Ying, and Noorhaniza Wahid (2012) [21] proposed a new hybrid intrusion detection system by using intelligent dynamics warm based roughest (IDS-RS)for feature selection and simplified swarm optimization for intrusion data classification. IDS-RS was proposed to select the most relevant features that can represent the pattern of the network traffic. In order to improve the performance of SSO classifier, a new weighted local search (WLS) strategy incorporated in SSO was proposed. The purpose of this new local search strategy was to discover the better solution from the neighborhood of the current solution produced by SSO.

Thaseen, IkramSumaiya, and Cherukuri Aswani Kumar (2017) [22] proposed an intrusion detection model using chi-square feature selection and multi class support vector machine (SVM). A parameter tuning technique was adopted for optimization of Radial Basis Function kernel parameter namely gamma represented by 'ϒ' and over fitting constant 'C'. These are the two important parameters required for the SVM model. The main idea behind this model was to construct a multi class SVM which has not been adopted for IDS so far to decrease the training and testing time and increase the individual classification accuracy of the network attacks. The investigational results on NSL-KDD dataset which was an enhanced version of KDDCup 1999 dataset shows that the proposed approach results in a better detection rate and reduced false alarm rate.

Çavuşoğlu, Ünal (2019) [23] developed a hybrid and layered Intrusion Detection System (IDS) that uses a combination of different machine learning and feature selection techniques to provide high performance intrusion detection in different attack types. In the developed system, initially, data preprocessing was performed on the NSL-KDD dataset, then by using different feature selection algorithms, the size of the dataset was reduced. Two new approaches have been proposed for feature selection operation. The layered architecture was created by determining appropriate machine learning algorithms according to attack type. Performance tests such as accuracy, DR, TP Rate, FP Rate, F-Measure, MCC and time of the proposed system are performed on the NSL-KDD dataset.

Aswani, Reema et al., (20-17) [24] introduced a hybrid artificial bee colony approach integrated with k-nearest neighbors to identify and segregate buzz in Twitter. A set of metrics comprising of created discussions, increase in authors, attention level, burstiness level, contribution sparseness, author interaction, author count and average length of discussions are used to model the buzz. The proposed approach considers the buzz discussions as outliers deviating from the normal discussions and identifies the same using the proposed hybrid bio inspired approach. Findings may be useful in domains like e-commerce, digital and influencer marketing to explore the factors that might create buzz along with the difference between the impact of buzz and normal discussions on the consumers.

3. Intrusion Detection Model

Over the last two decades, computer threats and cybercrimes have proliferated at the disadvantage of the general public, and newer threats are introduced each day that compromise the integrity, validity and confidentiality of data. Malicious activities in the internet are also known as intrusion.

Intrusion detection system (IDS) is software and hardware deployed to carry out the process of detecting unauthorized use of, or attack upon, a computer or a telecommunications network which is supposed to bridge the gaps in firewall and anti-viruses. An IDS provides monitoring [25] and analysis of user and system activity, can audit system configuration and vulnerabilities, assess the integrity of critical system and data files, provide statistical analysis of activity patterns based on the matching with known attacks, analyze abnormal activity, and operate system audit.

One advantage of the IDS is its ability to document the intrusion or threat to an organization, thereby providing bases for informing the public regarding the latest attack patterns through system logs. The proposed IDS model is the integration of K means-based ANN and PSO. Initially the features of the intruded networks are extracted from a benchmark dataset and it was trained to the proposed classifier. But it is difficult to find the number of clusters and the detection accuracy will be maximum if the number of clusters equal to the number of data types in the

dataset. This problem is formulated as a multi-objective function in PSO which optimally finds the cluster numbers that maximizes the detection accuracy and lower the false negatives.

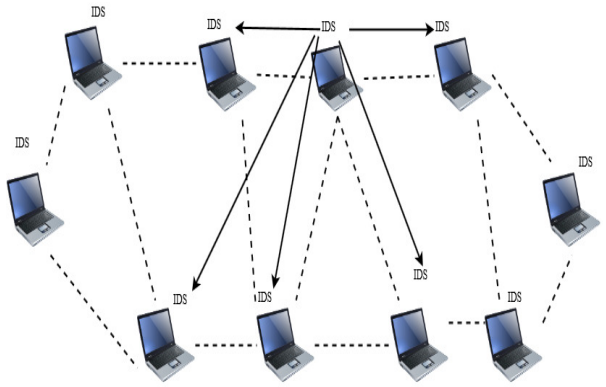

Figure 1: The IDS Architecture for Wireless Ad-Hoc Network

4. Proposed IDS Model

The study integrates artificial intelligence and machine-learning techniques with k-means data mining algorithm to develop an IDS [26] model with higher efficiency and lower false negatives. A common problem shared by current IDS is the high false positives and low detection rate. In the proposed work, we integrate the advantage of Artificial intelligence and machine learning techniques to overcome this issue. The proposed IDS model uses K-means algorithm based Artificial Neural Network (ANN) [27] integrated with Particle swarm optimization (PSO) algorithm [28] to increase the efficiency rate.

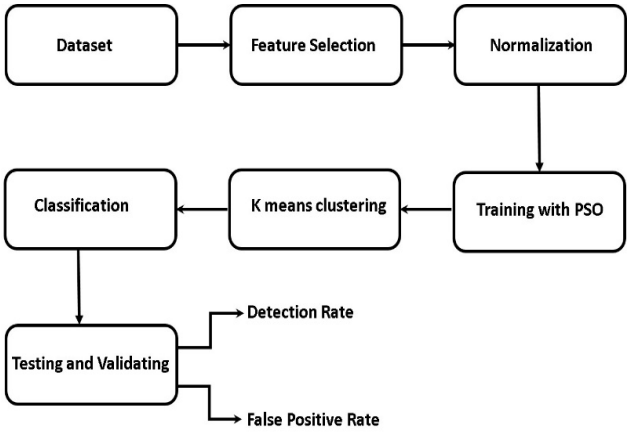

Figure 2: Proposed Block Diagram

4.1. Pre-processing

Pre-processing involves cleaning the data of inconsistencies and/or noise and combining or removing redundant entries. Pre-processing also involves converting the attributes of the dataset into numeric data and saving in a format readable because k-means works only on numerical data.

4.2. Feature Extraction [29]

After pre-processing the initial data, the useful information's or features from each data are extracted. We employed the simple features (attributes) that are extracted from the header's area of the selected network packets. These intrinsic features are available in many networks, for example, the duration (length of the connection), source host, destination host, source interface, and destination interface. We also used three features in each 2 seconds time interval:

- Total number of packets sent from and to the given interface in the considered time interval,
- Total number of bytes sent from and to the given interface in the considered time interval,
- Number of different source- destination pairs matching the given hostname-interface that are observed in the considered time interval.
- The number of packets and bytes allows to detect anomalies in traffic volume, and the third features allows detecting the network and the interface scans as well as the distributed attacks, which both result in an increased number of source-destination pairs.
- An efficient classifier further utilizes the extracted features in order to detect Intrusion present in the network.

4.3. K-Means Clustering Algorithm

Clustering is the method of grouping objects into meaningful subclasses so that the members from the same cluster are quite similar, and the members from different clusters are quite different from each other. Until now, the clustering algorithms can be categorized into four main groups partitioning algorithm, hierarchical algorithm, density-based algorithm and grid-based algorithm. Partitioning algorithms construct a partition of a database of N objects into a set of K clusters. Usually they start with an initial partition and then use an iterative control strategy to optimize an objective function. K-means represents a type of useful clustering techniques by competitive learning, which is also proved promising techniques in intrusion detection. K-Means is one of the simplest unsupervised learning algorithms that solve the clustering problem. The objective is to classify a given data set into a certain number of clusters (assume initial clusters) fixed a priori.

Algorithm 1 The pseudo code for the adapted K-Means clustering

1. Choose random k data points as the initial Cluster Centroids.
2. Repeat
3. For each data point x from D
4. Then compute the distance of x from each cluster mean (centroid)
5. Assign x to the nearest cluster.
6. End for loop.
7. Again compute the mean for current cluster collections.
8. Until reaching stable cluster
9. Use these centroids for normal and anomaly traffic.
10. Calculate the distance of centroid from normal and anomaly centroid points.
11. If distance$(d, Dm) >= 5$
12. Then anomaly found, exit 2.
13. Else 3.
14. d is a normal and it is not an Intrusion;

K-means clustering module can be summarized as follows:

$$K = \sum_{m=1}^{x} \sum_{n=1}^{y} \left\| d_n^{(m)} - c_m \right\| \quad (1)$$

$\left\| d_n^{(m)} - c_m \right\|$is a chosen distance measure between a data point and the cluster centroid, is an indicator of the distance of the n data points from their respective cluster Centroids. In order to apply the K-means algorithm to intrusion detection system, we design and realize the K-means algorithm analyze module, the graph shows the process flow:

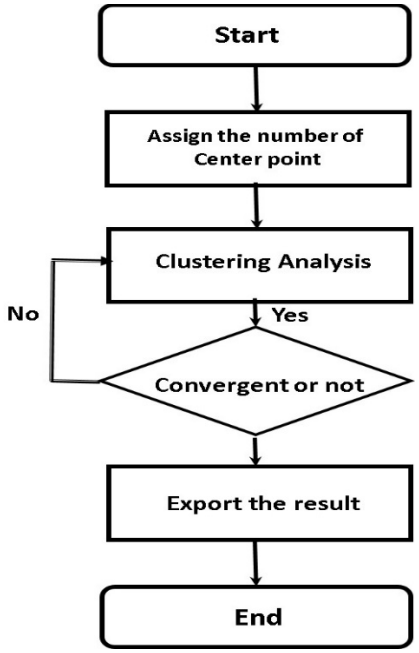

Figure 3: Working flow for K- means Algorithm

4.4. Review of Artificial Neural Network [30]

Feed forward neural network training is usually carried out using the called back propagation algorithm. Training the network with back propagation algorithm results in a non-linear mapping between the input and output variables. Thus, given the input/output pairs, the network can have its weights adjusted by the back propagation algorithm to capture the non-linear relationship. After training, the networks with fixed weights can provide the output for the training the network is based on the minimization of an energy function representing the instantaneous error.

ANN analysis was carried out using software Easy NN version 8.01. The network software uses back propagation algorithm and logistic function as activation function. The ANN used has three layers: an input layer that consists of five nodes (variables), one hidden layer consisting of five hidden nodes and an output layer that has one output node. To train an ANN model, a set of data containing input nodes and output nodes are fed. Once the training is over, ANN is capable of predicting the output when any input similar to the pattern that it has learned is fed. The ANN is tested for the remaining set of experimental data. The learning rate and momentum value of the network is set to optimize with a targeted error value of 0.05.

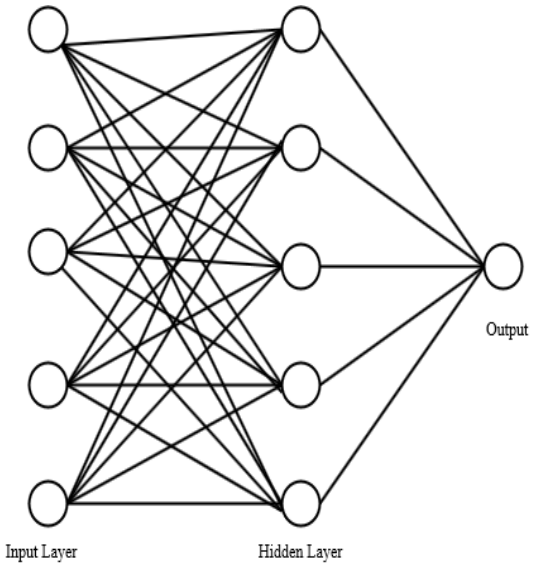

Figure 4: Schematic diagram of artificial neural network

4.5. K-Means based ANN-PSO

For implementation of ANN algorithm on the dataset, training data is divided into several subsets using k-means clustering technique. Subsequently, it trains different ANN using different subsets. Then, it determines membership grades of all these subsets and combines them using a new ANN to get final results. The whole framework of K-Means ANN is illustrated in Fig. 1. As typical machine learning framework, K-Means ANN incorporates both the training phase and testing phase.

Algorithm 2 The pseudo code for the adapted K-Means ANN

1. Start
2. Get the input features and Initialize the neural network parameters.
3. Define the relationships between input and output.
4. Divide the input for testing and training.
5. Train ANN using the training set.
6. Execute the Neural Network for the testing set.
7. Set j=1;
8. While(j<x)
9. Cluster the ANN outputs into K-clusters.
10. Calculate the weight of each cluster.
11. Calculate the error between the target output and ANN estimated output.
12. Increase j by 1.
13. Calculate false negatives.
14. End

The results of K-means ANN is optimized using PSO. In PSO, each particle is a point of N-dimensional solution space and has a speed$(N - dimensional\ vector)$. Different particle has individual fitness associated with objective function. Each particle adjusts their flight path according to its flying experience and flying experience of group and move closer to optimal point. The position of i-particle is denoted as,$X_i = (x_{i1}, x_{i2} \ldots . x_{iN})$ Flight speed is denoted as: $V_i = (v_{i1}, v_{i2} \ldots . v_{iN})$the best position which $i$particle passed is denoted as$P_{ibest} = (p_{i1}, p_{i2} \ldots . p_{iN})$the

groups' best position which it can get is denoted as $G_{best} = (g_1, g_2 \ldots . g_N)$. Particle Swarm has two primary operators: Velocity update and Position update. During each generation each particle is accelerated toward the particles previous best position and the global best position. At each iteration a new velocity value for each particle is calculated based on its current velocity, the distance from its previous best position, and the distance from the global best position. The new velocity value is then used to calculate the next position of the particle in the search space. This process is then iterated a set number of times or until a minimum error is achieved. In each step, according to PSO algorithm formula, which is proposed by Kenddy, particles update their velocity and position according to the following formula:

$$V_i(t) = wV_i(t-1) + C_1 r_1\big(P_i - X_i(t-1)\big) + C_2 r_2\big(G - X_i(t-1)\big) \quad (2)$$

$$X_i(t) = X_i(t-1) + V_i(t-1) \quad (3)$$

C_1 And C_2 denote accelerating factor. According to the experience of PSO algorithm, they are usually set$C_1 - C_2 = 2$. r_1 and r_2 are two random number between zero and one, w is called inertia weight. Researchers often use a constant V max to limit the speed of particles and improve search results. W plays a role which balance global search ability and local search ability. It is essential for the success of the algorithm. Shi and Eberhart, study on the effect of the W for optimize performance. They found that the larger the W is, the more easily escape from local minima, and the smaller the W is, the more favorably algorithm converges. Then they present a method, which makes inertia weight decrease linearly according to number of iterations.

In the beginning algorithm uses large inertia weight, it has a strong overall search capability. The later smaller inertia weight is used, and local search ability is improved. W is calculated as follows:

$$w = (w_1 - w_2) * \frac{Max_i - 1}{Max_i} + w_2 \quad (4)$$

w_1 and w_2 are the initial value and final value of inertia weight. Max_i and i are the maximum number of iterations and the current number of iterations for the algorithm, W reduces from 0.9 to 0.4 with the conduct of iteration. The objective function for PSO is set as

$$f(x) = \max\left(\frac{Detection\ Accuracy}{False\ Negatives}\right) + \max\,(1/Time) \quad (5)$$

The PSO algorithm proceeds as follows:

Algorithm 3 The pseudo code for the adapted PSO

1. Begin
2. Initialize the total number, velocity and position of the particles.
3. Calculate pbest and gbest.
4. Calculate the objective function.
5. Update the velocity and position of the particle.
6. Update pbest and gbest .
7. Repeat the steps until the termination condition reached.
8. End

5. Performance Analysis

NSL-KDD dataset is an improved version of the popular KDD Cup'99 dataset. It solves some inherent problems of the KDD'99 dataset (Tavallaee et al. 2009; McHugh 2000).Due to lack of public datasets for network-based IDS, the current version of NSL-KDD may be applied as an effective benchmark dataset for this work. Furthermore, major improvements are carried out on KDD'99 to obtain NSL-KDD and this is more advantageous over KDD'99. The number of instances in the NSL-KDD train and test sets is reasonable, which makes experimentation bias less by running experiments on whole dataset instead of running on randomly selected short portion of KDD'99 dataset. It is free of redundant records in train and test dataset, so the classifiers will not be biased towards repeated instances in the dataset.

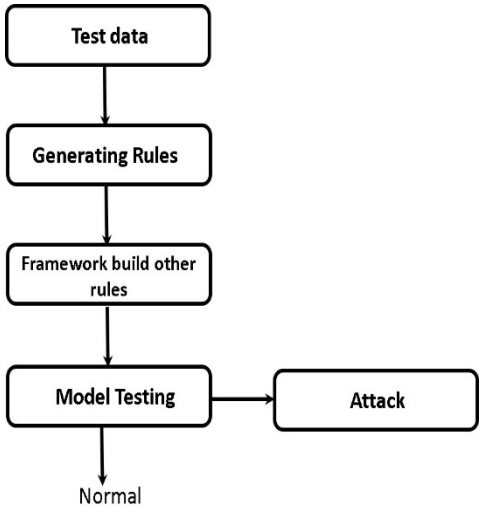

Figure 5: Implementation Setup Model

The NSL-KDD dataset contains two different files for training and testing, and hence, there is no overhead of dividing the dataset into training and testing which also makes a slight contribution towards performance evaluation of the learning techniques.

Table 1: Datasets with Attributes

Dataset	No. of records	No of attributes
KDDTrain+.txt	125,973	42
KDDTest+.txt	22,544	42

Table1shows the properties of the NSL-KDD train and test datasets (both are obtained as .txt files). It should be noted that there are no missing values in any attribute, and number of attributes in the table includes a class attribute. One approach during the training phase refers to processing of all the patterns or instances present in the KDDTrain+.txt dataset. However, size of testing set is 15% of size of whole dataset. Since these datasets are large and computation in ordinary machines might take too much time or sometimes might not support the memory requirements, randomly chosen 10% of the training dataset was used during training. The random selection of 10% of the training dataset was repeated for different executions so that there would be comparatively less chance of repeating the training data in different simulations. There are different types of attacks in the

dataset. However, in this work, it is considered as a two-class problem where patterns may belong to either 'normal' or 'anomaly' class.

5.1 Normalization of dataset

In the NSL-KDD datasets, the values for each attribute are often not distributed uniformly. It is wise to maintain a uniform distribution of each input attributes in the dataset before processing in the neural network. Hence, to ensure that the input values were compatible despite significant differences in their values, the dataset is normalized with respect to each input value where$d_i$the original value is;$d_{max}$and$d_{min}$are the maximum and minimum value, respectively, in the input attribute from whichdiis obtained. Then, normalized value of$d_i$is denoted as$d_i^{'}$. However, it was seen that the normalized dataset some-times contained majority of zeros and in such cases, it was preferred to use the in-built data normalization function of MATLAB called *mapminmax, which* normalizes data in the range$[-1,1]$.

$$d_i^{'} = \frac{d_i - d_{min}}{d_{max} - d_{min}} \quad (6)$$

5.1.1 Testing and Validation

For our experiments, we are using NSL-KDD dataset. NSL-KDD contains 42 fields as an attribute. In our algorithm, we have taken selected features. The performances of each method are measured according to,

- Accuracy
- False Positive Rate

A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. Although this type of error may not be completely eliminated, a good system should minimize its occurrence to provide useful information to the users. A false-negative occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior. While the true-positives (TP) and true-negatives (TN) are correct classifications. Recall Rate measures the proportion of actual positives that are correctly identified.

a. Accuracy

$$accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (7)$$

Where FN is False Negative, TN is True Negative, TP is True Positive, and FP is False Positive

b. False Alarm Rate

The false positive rate is the number of normal connections that are misclassified as attacks divided by the number of normal connections in the data set.

$$False\ alarm = \frac{FP}{FP+TN} \quad (8)$$

5.1.2 Performance Comparison

The performance of the proposed IDS model is compared with the performance of the K-means algorithm and K-means based ANN algorithm in this section in terms of accuracy and false alarm rate.

Figure 6 shows the accuracy comparison between proposed IDS model with K-means algorithm and K-means based ANN algorithm.

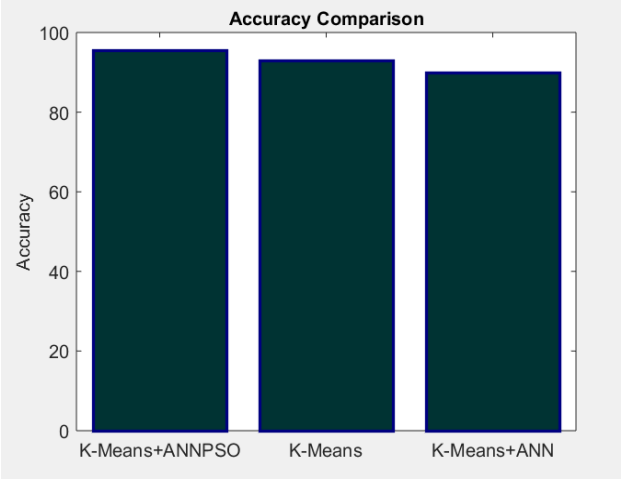

Figure 6: Accuracy comparison between existing techniques

Figure 6 shows the accuracy of proposed IDS model is 88.2321% and the K-means algorithm attains 85% accuracy and K-means based ANN algorithm attains 83% accuracy with NSL-KDD dataset. This shows the significance of the proposed IDS model than the existing IDS models.

Figure 7 shows the false alarm rate comparison between proposed IDS model with K-means algorithm and K-means based ANN algorithm.

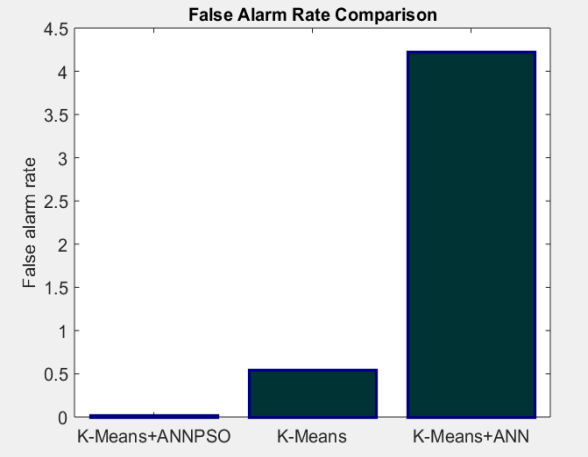

Figure 7: False Alarm Rate Comparison between existing techniques

Figure 7 shows the false alarm rate of proposed IDS model is ranging between 0-0.5 and the K-means algorithm attains false alarm rate of 0.5 and K-means based ANN algorithm attains maximum false alarm rate above 4 with NSL-KDD dataset. The significant reduce in false alarm rate shows the proposed IDS model is efficient.

6. Conclusion

Intrusion Detection is a process of detecting Intrusion in a computer system in order to increase the security. Intrusion detection is an area in which more and more sensitive data are stored and processed in networked system. After reading several research works, we come with several advantage and disadvantage. In this paper, a novel method for Intrusion detection was proposed. The proposed Intrusion detection system combines the advantages of machine learning and artificial intelligence to overcome the general issues present in the intrusion detection systems. Using the PSO algorithm, a multi-objective problem is formulated to find the optimal clusters and the issue is solved. The proposed system is tested in NSL-KD dataset and it achieved maximum detection accuracy of 88%. In addition to this, it is observed that the false negative rate of the proposed IDS is significantly reduced when compared with the results obtained with K-means algorithm and K-means based ANN algorithm.

References

[1] Sobh, Tarek S. "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art." Computer Standards & Interfaces 28, no. 6 (2006): 670-694.

[2] Aydın, M. Ali, A. Halim Zaim, and K. GökhanCeylan. "A hybrid intrusion detection system design for computer network security." Computers & Electrical Engineering 35, no. 3 (2009): 517-526.

[3] Raymond, Jean-François. "Traffic analysis: Protocols, attacks, design issues, and open problems." In Designing Privacy Enhancing Technologies, pp. 10-29. Springer, Berlin, Heidelberg, 2001.

[4] Tsai, Chih-Fong, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. "Intrusion detection by machine learning: A review." expert systems with applications 36, no. 10 (2009): 11994-12000.

[5] Debar, Hervé, Marc Dacier, and Andreas Wespi. "A revised taxonomy for intrusion-detection systems." In Annales des télécommunications, vol. 55, no. 7-8, pp. 361-378. Springer-Verlag, 2000.

[6] Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36, no. 1 (2013): 16-24.

[7] Patcha, Animesh, and Jung-Min Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer networks 51, no. 12 (2007): 3448-3470.

[8] Depren, Ozgur, Murat Topallar, EminAnarim, and M. Kemal Ciliz. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks." Expert systems with Applications 29, no. 4 (2005): 713-722.

[9] Labib, Khaled, and V. Rao Vemuri. "An application of principal component analysis to the detection and visualization of computer network attacks." In Annales des télécommunications, vol. 61, no. 1-2, pp. 218-234. Springer-Verlag, 2006.

[10] Verwoerd, Theuns, and Ray Hunt. "Intrusion detection techniques and approaches." Computer communications 25, no. 15 (2002): 1356-1365.

[11] Syarif, Iwan, Adam Prugel-Bennett, and Gary Wills. "Unsupervised clustering approach for network anomaly detection." In International conference on networked digital technologies, pp. 135-145. Springer, Berlin, Heidelberg, 2012.

[12] Jiang, ShengYi, Xiaoyu Song, Hui Wang, Jian-Jun Han, and Qing-Hua Li. "A clustering-based method for unsupervised intrusion detections." Pattern Recognition Letters 27, no. 7 (2006): 802-810.

[13] Fan, Cheng, Fu Xiao, Yang Zhao, and Jiayuan Wang. "Analytical investigation of autoencoder-based methods for unsupervised anomaly detection in building energy data." Applied energy 211 (2018): 1123-1135.

[14] Aggarwal, Charu C., and S. Yu Philip. "Data mining techniques for associations, clustering and classification." In Pacific-Asia Conference on Knowledge Discovery and Data Mining, pp. 13-23. Springer, Berlin, Heidelberg, 1999.

[15] Stewart, Theo J. "A critical survey on the status of multiple criteria decision making theory and practice." Omega 20, no. 5-6 (1992): 569-586.

[16] Abraham, Ajith, Swagatam Das, and Sandip Roy. "Swarm intelligence algorithms for data clustering." In Soft computing for knowledge discovery and data mining, pp. 279-313. Springer, Boston, MA, 2008.

[17] Zhang, Zhongxing, and Baoping Gu. "Intrusion detection network based on fuzzy c-means and particle swarm optimization." In Proceedings of the 6th International Asia Conference on Industrial Engineering and Management Innovation, pp. 111-119. Atlantis Press, Paris, 2016.

[18] Patel, Ahmed, Mona Taghavi, KavehBakhtiyari, and Joaquim CelestinoJúNior. "An intrusion detection and prevention system in cloud computing: A systematic review." Journal of network and computer applications 36, no. 1 (2013): 25-41.

[19] Folino, Gianluigi, and Pietro Sabatino. "Ensemble based collaborative and distributed intrusion detection systems: A survey." Journal of Network and Computer Applications 66 (2016): 1-16.

[20] Sharma, Ruby, and Sandeep Chaurasia. "An enhanced approach to fuzzy C-means clustering for anomaly detection." In Proceedings of First International Conference on Smart System, Innovations and Computing, pp. 623-636. Springer, Singapore, 2018.

[21] Chung, Yuk Ying, and Noorhaniza Wahid. "A hybrid network intrusion detection system using simplified swarm optimization (SSO)." Applied Soft Computing 12, no. 9 (2012): 3014-3022.

[22] Thaseen, IkramSumaiya, and CherukuriAswani Kumar. "Intrusion detection model using fusion of chi-square feature selection and multi class SVM." Journal of King Saud University-Computer and Information Sciences 29, no. 4 (2017): 462-472.

[23] Çavuşoğlu, Ünal, Shirin Panahi, AkifAkgül, SajadJafari, and SezginKaçar. "A new chaotic system with hidden attractor and its engineering applications: analog circuit realization and image encryption." Analog Integrated Circuits and Signal Processing 98, no. 1 (2019): 85-99.

[24] Aswani, Reema, S. P. Ghrera, Arpan Kumar Kar, and Satish Chandra. "Identifying buzz in social media: a hybrid approach using artificial bee colony and k-nearest neighbors for outlier detection." Social Network Analysis and Mining 7, no. 1 (2017): 38.

[25] Duque, Solane, and Mohd Nizam bin Omar. "Using data mining algorithms for developing a model for intrusion detection system (IDS)." Procedia Computer Science 61 (2015): 46-51.

[26] Benmouiza, Khalil, and Ali Cheknane. "Forecasting hourly global solar radiation using hybrid k-means and nonlinear autoregressive neural network models." Energy Conversion and Management 75 (2013): 561-569.

[27] Abd-El-Wahed, W. F., A. A. Mousa, and M. A. El-Shorbagy. "Integrating particle swarm optimization with genetic algorithms for solving nonlinear optimization problems." Journal of Computational and Applied Mathematics 235, no. 5 (2011): 1446-1453.

[28] Hart, Christopher G., and Nickolas Vlahopoulos. "An integrated multidisciplinary particle swarm optimization approach to conceptual ship design." Structural and Multidisciplinary Optimization 41, no. 3 (2010): 481-494.

[29] Lunt, Teresa F. "A survey of intrusion detection techniques." Computers & Security 12, no. 4 (1993): 405-418.

[30] Manohar, Balaraman, and SoundarDivakar. "An artificial neural network analysis of porcine pancreas lipase catalysed esterification of anthranilic acid with methanol." Process Biochemistry 40, no. 10 (2005): 3372-3376.