Indian Journal of Science and Technology, *Vol 8(34), DOI: 10.17485/ijst/2015/v8i34/76697, December 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Improved Hybrid Fuzzy Jordan Network and Artificial Neural Network for Robust and Efficient Intrusion Detection System

A. Dhivya[1*] and S. N. Sivanandam[2]

[1]Department of Computer Science and Engineering, Karpagam University, Coimbatore - 641042, Tamil Nadu, India; adhivya123research@gmail.com
[2]Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore - 641042, Tamil Nadu, India; sivanandanresearch@gmail.com

Abstract

Objective: The main objective of this paper is to improve the intrusion detection accuracy of neural networks by hybridized with Jordan network, applying novel Lyapunov function and changing input values as fuzzy values using fuzzy logic. **Methods:** In this research, the intrusion detection of NSL KDD dataset is carry out by neural network first . The performance of neural networks mainly depends on the parameters like number of hidden layer, no of node in the hidden layer and the no of epoch. Selecting the proper parameters values and weight initialization are the main difficulty in neural network. To overcome this issue a hybrid network by combining neural network with Jordan network is proposed which is highly sensitive to weight convergence. In hybrid network Lyapunov function is used to achieve the stability of equilibrium between two networks. But in this work a novel Lyapunov function is proposed to achieve global robust stability in hybrid network. A novel Lyapunov function uses a class of general activation functions which are not to be differentiable, bounded or monotonically nondecreasing. A set of criteria are derived to guarantee the existence, uniqueness and global robust stability of the equilibrium of hybrid networks with time delays. Then the learning ability of hybrid network is improved by using fuzzy logic. The hybrid network improved by a novel Lyapunov and fuzzy logic is called as Improved Fuzzy Hybrid Jordan network and Artificial Neural Network (IHFJANN). **Findings:** Artificial Neural Network (ANN), Hybrid Jordan network and Artificial Neural Network (HJANN) and Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (IHFJ ANN) are applied on NSL KDD training dataset to lean the type of available attacks. NSL training dataset contains 2500 instances and 38 attributes where as testing dataset contains 995 instances and 38 attributes. The learned model of three classifiers is used to predict the classes in test dataset. The performance measures are evaluated in terms of accuracy, precision, recall and f-measure values. **Improvement:** The classification accuracy of Artificial Neural Network (ANN), Hybrid Jordan network and Artificial Neural Network (HJANN) and Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (IHFJANN) are 72%, 80% and 84% respectively. Accuracy is increased by 12% in IHFJANN than the ANN and 4% than the HJANN. The precision value of ANN, HJANN and IHFJANN are 0.46, 0.54 and 0.57 respectively. Precision value is increased by 0.9 in IHFJANN than the ANN and 0.3 than the HJANN. The recall value of ANN, HJANN and IHFJANN are 0.73, 0.81 and 0.84 respectively. Recall value is increased by 0.9 in IHFJANN than the ANN and 0.3 than the HJANN. The F-measure value of ANN, HJANN and IHFJANN are 0.58, 0.65 and 0.68 respectively. F-measure value is increased by 0.10 in IHFJANN than the ANN and 0.3 than the HJANN. The results proved that the proposed IHFJANN provides better performance than ANN and HJANN.

Keywords: Global stability, hybrid fuzzy Jordan network and Lyapunov's function

1. Introduction

The intrusion detection system (IDS) examines all inbound and outbound network activities. IDS also recognize mistrustful patterns which specify a network attack from someone trying to break into or compromise a system. The intrusion detection techniques such as Artificial Neural Network (ANN) based intrusion detection, Fuzzy Logic (FL), Bayesian learning algorithm and Genetic Algorithms (GA) have been suggested in the

*Author for correspondence

preceding researches. ANN based intrusion detection is used to build the intrusion model based on the important features in order to achieve the better detection rate. Fuzzy logic[1] is to generate the fuzzy rules for detecting the intrusions effectively and also to handle the mixed attributes in the given dataset. Bayesian learning algorithm[2] is to build a behavior model which analyzes the system behavior efficiently and genetic algorithm[3] based IDS is to select the optimal features in a specified dataset for improving the intrusion classification performances.

Iftikhar Ahmad et.al[4] presented the Artificial Neural Network (ANN) that detects the probing attacks efficiently. The attack detection is essential to provide security to computers and network system. Even though, a number of attempts have been done in the attack identification area, they suffered various restrictions such as time consuming numerical analysis, regular updation, non adaptive, accuracy and flexibility. To avoid the above mentioned problems, this research used ANN method that supports an ideal specification of an attack discovery system. ANN can discover the attacks conducted against the network in a coordinated manner by multiple attackers, the ability to process data from a number of sources in a non-linear fashion. The advantage of ANN is that it is capable of analyzing the data from the network, even if the data is incomplete or unclear. The KDD cup 99 dataset is evaluated by using ANN which provides higher security against attacks. However it has issue with computational expensive and error rates.

Andrej Krenker et.al[5] presented the Jordan network to improve the network performances. Jordan network is multi layer perceptron with a set K so called as context neurons. In principle, a context neuron just memorizes an output until it can be processed in the next time step. Therefore, there are weighted connections between each output neuron and one context neuron. The stored values are returned to the actual network by means of complete links between the context neurons and the input layer. The back propagation training algorithm is applied to multilayered Jordan network for improving the weight convergence. The training and testing error values are reduced than the previous research algorithms. However Jordan network cannot access its own context and it takes long time for training process.

Dahlia Asyiqin et.al[4] presented a hybrid Neuro – Fuzzy based Intrusion Detection System. Initially data set is divided into training set and testing set. The training sets are created using fuzzy clustering. Then it is trained using ANN model. Then all selective training set is used in the next simulation to reduce the error. Based on the membership grades, training another new ANN is done to combine the results. Results had guaranteed that the hybrid approach performed better detection especially for low frequent over NSL dataset compared to original KDD dataset, due to the removal of redundancy and incomplete elements in the original dataset. However the convergence speed is slow in this method.

To avoid the issues in ANN, Jordan network and hybrid networks, in this research we propose Hybrid Jordan network and ANN (HJANN) and Improved Hybrid Fuzzy Jordan network and ANN (IHFJANN) networks. The main purpose of this research is to improve the accuracy of intrusion detection by applying the novel Lyapunov function and using fuzzy logic for changing the input values.

Gang Wang et.al[6] suggested a new approach to intrusion detection using Artificial Neural Networks (ANN) and fuzzy clustering. To improve the intrusion detection performance, in this research the method named as Fuzzy Clustering ANN (FC-ANN) is introduced. Fuzzy clustering method is used to generate various training subsets. Consequently, based on different training subsets, different ANN models are trained to formulate different base models. The fuzzy clustering method is used to divide the heterogeneous training set into several homogeneous subsets. Thus complexity of each sub training set is reduced and consequently the detection performance is increased. However this research has issue with finding the appropriate number of clustering.

Shingo Mabu et.al[7] suggested an intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming. By combining fuzzy set theory with genetic network programming (GNP), this research can deal with mixed database which contains both discrete and continuous attributes. The GNP for association rule mining is built for rule extraction process and fitness function is used to increase the classification accuracy values. This approach is effectively useful for both anomaly and misuse detection along with specified classifiers. For misuse detection, the normal-pattern rules and intrusion-pattern rules are extracted, while for anomaly detection only the normal-pattern rules are extracted. Therefore, many rules extracted by GNP cover the spaces of the classes widely. However the algorithm has high computational complexity.

L. A. Mozelli et.al[8] recommended novel Lyapunov's function along with fuzzy system concept. This research

provides improved stability constraints fuzzy systems using novel Lyapunov's function. It is used to aggregate more information with respect to time derivative variation through augmented state vector. The test conditions attained from this novel are derived by extra null terms and enclose the time derivative information. Another research[4] described the Lyapunov-Krasovskii functions creation through novel approaches. This method is used for leading the efficient stability constraints. However this research scenario has issue with conservatism as well as maximal permission of delay for gradually moment differing delays.

P. Srinivasu et.al[9] introduced a genetic algorithm based weight extraction algorithm for artificial neural network classifier in intrusion detection. The proposed system has three phases. They are pre-processing, weight extraction and classification. In pre-processing phase, the unnecessary noise is removed. In weight extraction phase, the individuals are denoted such that every individual chromosome consists of number of genes presenting the weights of the neural network. The weight function is extracted by using genetic algorithm. An artificial neural network compact with the process of simulating the behaviour of biological neurons is carried out in classification phase to offer an efficient means to handle classification troubles. However optimal method is needed for reducing iterations.

Saurabh Mukherjeea et.al[10] introduced an Intrusion Detection scheme which is based on the Naive Bayes Classifier with Feature Reduction. In order to identify reduced input features in building IDS the feature vitality based reduction technique is used, which is computationally efficient and effective. The naïve Bayes classifier operates on a strong independence assumption and the probability of one attribute does not affect the probability of the other. The reduced data sets are classified by using general naïve bayes classifier on discretized values. Since results using discretized features are usually more compact, shorter and accurate than using continuous values. However it has huge overhead and complexity.

S. Ganapathy et.al[11] presented a novel weighted fuzzy c-means clustering with genetic algorithm to determine the proper cluster structures. The immune genetic algorithm is utilized in the approach for improving the classification accuracy by selecting the optimal features. The main purpose of this approach is that it uses clustering to identify the anomaly intrusion and classify both signature and anomaly intrusions. The weighted fuzzy c-means clustering with genetic algorithm is to build the network which is more accurate for attack detection to improve the network performance. This approach also improves the prediction accuracy, stability and overcomes high dimensionality problem. However still it needs improvement in detection accuracy by using intelligent agent for decision making.

Reda M. Elbasiony et.al[12] presented hybrid network intrusion detection using random forest and weighted k-means algorithms. In misuse detection, random forests classification algorithm is used to build intrusion patterns and in anomaly detection, the k-means clustering algorithm is used to detect novel intrusions by clustering the network connections. In the hybrid framework, weighted k-means algorithm is used to solve the problem of mixed attribute features by using random forest algorithm. It overcomes the issues of both anomaly and misuse detection methods. Important feature values are computed by random forest which is used in misuse detection and improves the detection rate of anomaly detection. It is used to improve the anomalous cluster determination by injecting known attacks into the uncertain data. However it has issue with speed of convergence.

Wafa Alsharafat[13] discussed Artificial Neural Network (ANN) and extended classifier method for network intrusion detection. To avoid the cyber attacks, intrusion detection method is important for defending information system security. The main purpose of this research is to recognize significant features for building the intrusion detection system and it is used to improve the better detection rates. The ANN is used in filtering the unnecessary features and combines the best set of features for every type of network attacks. The extended classifier is developed in this research to achieve better detection rates. However still it has issue with false positive rates.

Monowar H. Bhuyan et.al[14] discussed the network anomaly detection which reduces the computational complexity of training dataset. In this research, there are two standard criteria to classify and evaluate the network intrusion detection systems such as detection strategy as well as evaluation datasets. This research also presented several detection methods, systems and tools. Several evaluation criteria are discussed for testing the performance of a detection method. However it has issue with false rates and leads to poor system performance.

Zebardast B, Maleki I and Maroufi A[15] presented a novel multilayer perceptron artificial neural network for improving the classification accuracy. The Radial Basis Function (RBF) artificial neural network is combined

with k means clustering and genetic algorithm to progress the efficiency and reduce the error rates. Gharehchopogh F S, Ebrahimi L, Maleki I and Gourabi S J[16] discussed the ambiguity problems and reliability issues in software development. To improve the accuracy of cost estimation model, novel particle swarm optimization (PSO) with hybrid of fuzzy c means algorithm is used. To avoid the drawbacks of preceding research works, we propose fuzzy hybrid networks in this research.

2. Hybrid Jordan Network and Artificial Neural Network (HJANN)

In this section, Hybrid Jordan network and Artificial Neural Network (HJANN) based novel Lyapunov Global Robust Stability function are introduced for improving the convergence speed and progressing the analysis of global robust stability. The Jordan network is a simple recurrent network improved by Michael I. Jordan in 1986. The context layer contains the preceding output from the output layer and then repeats that value to the hidden layer's input. The hidden layer obtains input from the prior iteration's output layer. The neural network is also improved by Jordan network with a recurrent constrained learning. It is focused on the proper parameter selection and weight initialization by combining the Jordan network with ANN. The proposed technique improves the accuracy and efficiency of identification of intrusions in the neural networks through the reduction of noise rate.

By the construction of the novel Lyapunov functions, several novel constraints are derived to guarantee the existence, distinctiveness and universal robust stability of the equilibrium of hybrid network systems along with time delays. Such kind of criterion does not need the activation functions which are to be diverse, bounded or monotonically non-decreasing. The stability of equilibrium is achieved among neural network and Jordan network by using hybrid network Lyapunov function. Lyapunov global robust stability function is parameterized by some parameters. The delayed neural network model is defined through the following state equations.

$$\frac{du_i(t)}{dt} = -c_i u_i(t) + \sum_{j=1}^{n} a_{ij} f_j(u_j(t)) + \sum_{j=1}^{n} b_{ij} f_j(u_j(t-\tau_{ij})) + l_i, \mathrm{i} = 1, 2, \ldots, \mathrm{n} \quad (1)$$

Where $c_i > 0$, n identifies the number of units in the neural network. $u_i(t)$ Corresponds to the state of the ith unit at a time t, $f_j(u_j(t))$ identifies the activation function of the jth unit at a time t, a_{ij}, b_{ij} and c_i are constants. c_i is indicating the rate along with ith unit and a_{ij} identifies the weight of the jth unit on the ith unit at time t. b_{ij} is representing the weight of the jth unit on the ith unit at time t – τ_{ij}. I_i is the outside bias on the ith unit, τ_{ij} is the time delay and $\tau_{ij} \geq 0$.

There are some essential data such as the values of neuron rates c_i(i = 1, 2, ….. n) and the weight coefficients a_{ij}, b_{ij}(i, j=1, 2, …..n). In general it is obtained and processed by using the statistical computation. Hence the estimation errors might be occur and the values of c_i, a_{ij}, b_{ij}(i, j = 1, 2, … n) has been deviated. The intrusions are discivered by using the deviation value in the neural network system robustly. Here the quantities of c_i, a_{ij}, b_{ij} (i, j = 1, 2, … n) is described as follows.

$$A = (b_{ij})_{n\times n} : \underline{B} \leq B \leq \overline{B}, i.e., \underline{b_{ij}} \leq b \quad (2)$$

By using the above mentioned equations (1) and (2), can improve the robust stability of delayed neural networks significantly.

3. HJANN – Architecture Diagram

The Hybrid Jordan network and ANN (HJANN) architecture is shown in Figure 1. It describes the three input layer, three hidden layer, two context layer and two output layer functions.

The main motivation of this research scenario is achieving the global robust stability of deferred neural networks along with a group of universal activation functions. A group of constraints are derived to guarantee the existence, exclusivity and global robust stability of the equilibrium of neural network systems along with time delays. The activation functions f_j(j = 1, 2, …, n) in system (1) assure the subsequent consideration.

(H_1) There occur some scalars $L_j > 0 (j = 1, 2, \ldots, n)$ such that

$$|f_j(u) - f_j(u)| \leq L_j|u - v| \text{ for all u, v} \in R \quad (3)$$

The above equation represents the activation functions fulfilled which is not essentially differentiable and bounded 14]. Lyapunov Global Robust Stability function is parameterized by some parameters. Consider (H_1), equation (1) and (2) is globally robust stable independent of time delays if there is positive constants $\lambda_1, \lambda_2, \ldots\ldots, \lambda_n$ such that

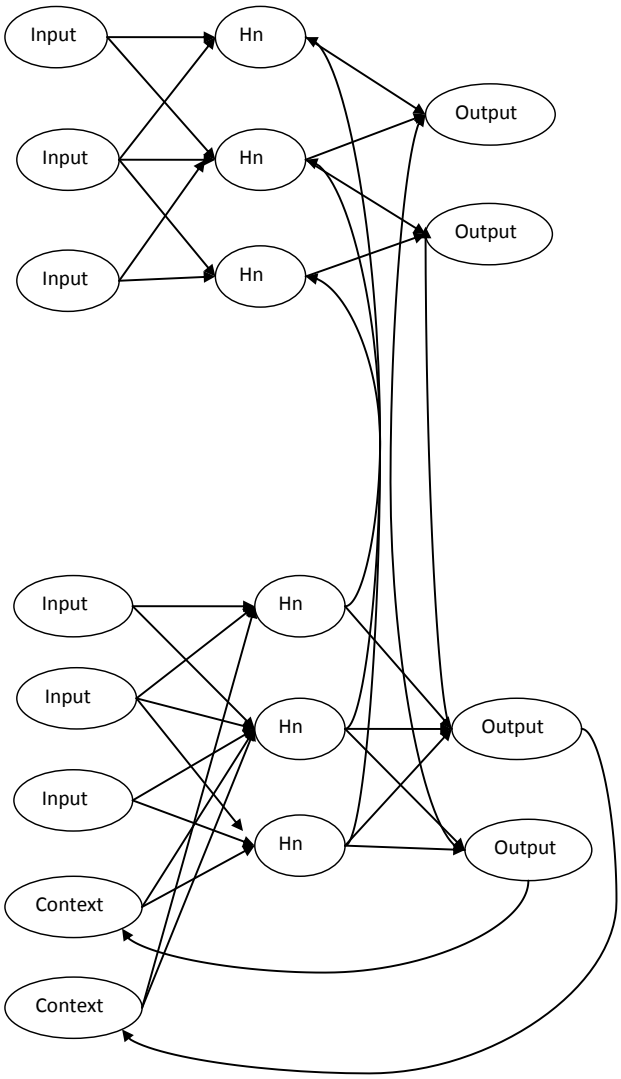

Figure 1. HJANN Architecture Diagram.

$$\lambda_i c_i > \sum_{j=1}^{n} \lambda_i a_{ij}^* L_j + \sum_{j=1}^{n} \lambda_j b_{ij}^* L_j \tag{4}$$

Where i = 1, 2, …, n, $a_{ij}^* = \max\{|a_{ij}|, \overline{a_{ij}}\}$, $b_{ij}^* = \max\{|b_{ij}|, \overline{b_{ij}}\}$,

And by the transformation, the equation (1) can be rewritten as following

$$\frac{dz_i(t)}{dt} = -c_i z_i(t) + \sum_{j=1}^{n} a_{ij}[f_j(z_j(t) + u_j^*) - f_j(u_j^*)] + \sum_{j=1}^{n} b_{ij}[f_i(z_j(t-\tau_{ij}) + u_j^*) - f_j(u_j^*)] \tag{5}$$

This can be proved, if u^* is equilibrium of system (1), then $(0, 0, \ldots 0)^T$ is equilibrium of system (5).

To demonstrate the neural system (1) along with (2) is globally robust stable, it is adequate to illustrate that the trivial solution of system (5) is globally stable.

Consider the $i_o = i_o(t)$ be the index such that $|\lambda_{i_o}^{-1} z_{i_o}(t)| = \max_{1\le i\le n} |\lambda_i(-1) z_i(t)|$. The novel global lyapunov function is constructed as given below.

$$V(t) = |z_{io}(t)| + \sum_{j=1}^{n} b_{i_o j}^* L_j \int_{(r-\tau i_{oj})}^{t} z_j(s)|ds \tag{6}$$

This novel Lyapunov global robust stable method is used to reduce the intrusions through this process efficiently and effectively. It aggregates their opinions about intrusions using Lyapunov function. While training and testing the specified dataset, it removes the intrusions globally. Hence it improves the performance as well as stability of the system significantly.

4. Improved Hybrid Fuzzy Jordan network and ANN (IHFJANN)

To improve the convergence Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (IHFJANN) is introduced. This system is adaptation of the concept of fuzzy with hybrid Jordan network and artificial neural network. The combination of fuzzy system with hybrid network is used for more accurate prediction and increasing the speed of the network. The purpose is to achieve a faster rate of convergence by controlling the learning rate parameter with fuzzy rules. IHFANN is maximizing the more accurate decision in the neural network applications.

The fuzzy logic control method is used to improve the learning parameters such as learning rate and momentum in the hybrid network. The use of fuzzy logic control is adjusts the learning rate and momentum based on the error rate. The set of rules are generated which reflects the usage of parameters to change the hybrid network's learning rate and momentum. IHFJANN provides high classification accuracy in KDD NSL intrusion dataset.

The IHFJANN algorithm is given below for increasing the hidden layer neurons depends on iterative training. It is used to establish an optimal or suboptimal weight initialization and number of hidden layer neurons in a Jordan network. The evaluation of fuzzy neural Jordan networks involves the five layers such as input layer, fuzzification layer, rule base layer, fuzzy outputs and output layer.

4.1 IHFJANN – Architecture Diagram

The Improved Hybrid Fuzzy Jordan Artificial Neural Network (IHFJANN) architecture is shown in Figure 2. It describes the number of input layers, number of hidden layer and number of output layer functions.

4.2 Algorithm

Formula Description

The output of neural network can be represented by

$$y(k) = v(k)\Phi(w(k), x(k)) \tag{7}$$

Where V(k) and W (k) is optimal and weight metrics respectively.

$$e(k) = [e_1(k) \ldots e_h(k)]^T \tag{8}$$

Where e (k) is error minimization function along with the output of hidden layer

$$\Phi(w(k), x(k) = [\Phi_1(k) \ldots \Phi_m(k)]^T \tag{9}$$

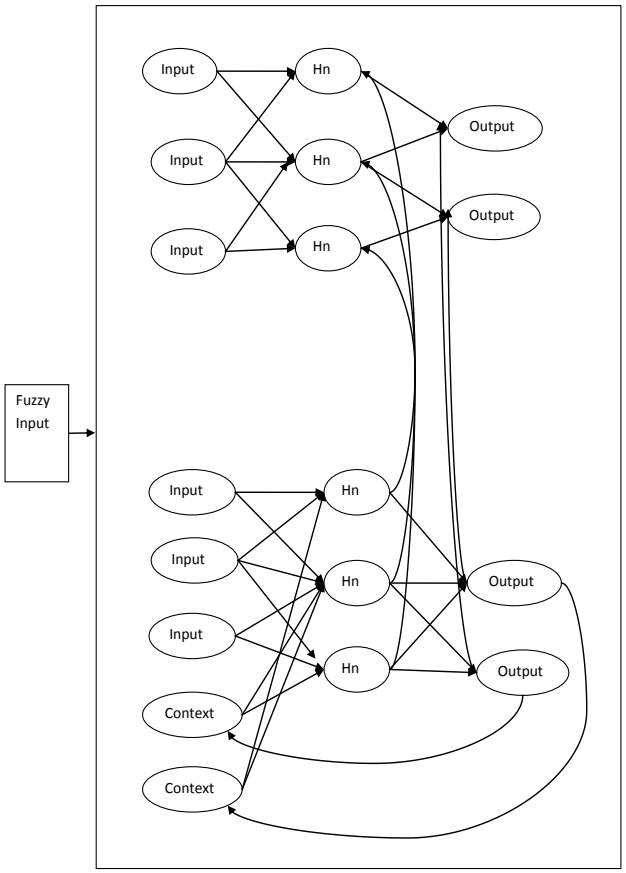

Figure 2. IHFJANN Architecture Diagram

The neural network

$$H_{iN}(k) = W_{iN}(k)x(k) \tag{10}$$

Where H_{iN} hidden input of is neural network and W_{iN} is weight value of neural network

Jordan network

$$H_{ij}(k) = W_{ij}(k)x(k) + c(k) \tag{11}$$

Where H_{ij} hidden input of is Jordan network, W_{ij} is weight value of Jordan network and c (k) is context

The neural control layer of hidden layer

$$\Delta^W(k+1) = \Delta^W(k) + \frac{\alpha^W(k)}{\rho^W(k)}||e(k) \tag{12}$$

Where Δ^W(k) is the adaptive dead zone estimate of the hidden layer

Output of hidden layer in neural network

$$H_{yN}(k) = W_{iNJ}(k) + c(y_j) \tag{13}$$

Where $W_{iNJ}(k)$ is weight value of neural and Jordan network, $c(y_i)$ is context of Jordan network output

Output of hidden layer in Jordan network

$$H_{yJ}(k) = W_{ij}(k) + c(y_j) \tag{14}$$

The errors or intrusions are reduced by the fuzzy function

$$e = \text{diff}(Y, D) = \frac{1}{2}\sum (y_1^{(a)} - d_1^{(a)})^2 + (y_2^{(a)} - d_2^{(a)})^2 \tag{15}$$

Where y is current output and d is desired output with fuzzy function.

HJANN output

$$H_{yN}(k) + H_{yJ}(k) = O(y)_{JN} \tag{16}$$

Where $O(y)_{JN}$ is hybrid output of neural network and Jordan network

Fuzzy logic input

$$F^l = \bigcap_{i=1}^{n} F_i^l \tag{17}$$

Where F_i^l is number of fuzzy input values satisfied by generated rules

IHFJANN output

$$F^l(H_{yN}(k) + H_{yJ}(k)) = O(y)_{FJN} \tag{18}$$

Where $O(y)_{FJN}$ is output of hybrid fuzzy Jordan and neural network

4.3 Algorithm Procedure

1. Begin with a comparatively small number of fuzzy neurons.
2. Selection is based on the previous knowledge of the neuron.
3. Set maximum weight-initialization.
4. Initialize the neural network and Jordan network with the associated random weight initialization for the output using (10) and (11)
5. Update the neural input vector x(k)
6. Compute the output of hidden in neural network $H_{yN}(k)$ using (13)
7. Compute the learning rates of each layer and update the weight matrices by using (12)
8. Compute the output of hidden in Jordan network $H_{yJ}(k)$ using (14)
9. Go to step 4 and continue until the end of the training data points.
10. Save the values for particular weight initialization step for the iterative training and continue until the maximum weight-initialization number is reached.
11. Hybrid the Jordan network with neural network and obtain the HJANN output using (16)
12. Obtain the resultant weight initialization as the most excellent value for the training based on the chosen number of fuzzy neurons.
13. Get the fuzzy input using (17) and obtain the hybrid fuzzy values in IHFJANN using (18)
14. The error rate is reduced significantly by using (15) and identified the more accurate results in terms of intrusions.

5. Results and Discussion

In this section the performance of existing and proposed scenarios are compared in terms of performance metrics. Elman Back Propagation artificial neural network algorithm is a prominent method to identify the intrusion detection. Radial Basis Function (RBF) is a kernel function and each neuron contains the RBF on a point along with many features. RBF network consists of two layers such as hidden layer and output layer. Input is mapped into each RBF in the hidden layer and RBF is used for increasing the speed of training data. The number of input attributes is 38 and 48 attributes for hidden layer. The output has four class labels in the dataset. The dataset considered in this research work is NSL KDD intrusion detection. The classification algorithm such as neural network is applied on the given NSL KDD dataset to analyze the various intrusions effectively. The class labels such as Denial of Attacks (DOS), probe, Remote to Local Attack (R2L) and User to Root Attack (U2R) are considered. The training dataset contains 2500 tuples and 38 attributes whereas the testing dataset contains 995 tuples and 38 attributes.

The methods are analyzed and the performance of neural networks is evaluated for intrusion detection. The Artificial Neural Network (ANN), Hybrid Jordan network and ANN (HJANN) and Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (IHFJANN) are compared to determine their efficiency. To increase the accuracy as well as efficiency the improved parameters are utilized in this scenario. From the experimental result we can conclude that proposed methodology is improves the prediction accuracy and also reduces the error rate significantly. Thus the proposed Improved Fuzzy Hybrid Jordan network and Artificial Neural Network (IHFJANN) is superior in the detection of intrusions and overall system performance.

5.1 Accuracy

Accuracy of the classification rate is measured with the values of the True Negative, True Positive, False Positive, False negative actual class and predicted class results. It is defined as follows,

$$\text{Accuracy} = \frac{\text{True positive} + \text{True negative}}{\text{True positive} + \text{True negative} + \text{False positive} + \text{False negative}}$$

From the Figure 3 it can be proved that the proposed methodology provides better result than the existing approach with increased accuracy values. In this graph, methods are plotted in the x axis and the accuracy values are plotted in the y axis. The accuracy value is low by using the existing methods of ANN and Hybrid Jordan network and ANN (HJANN). The accuracy value is significantly increased by using proposed method of Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (IHFJANN). From the experimental result we can conclude that proposed method is superior to existing system in terms of accuracy.

Table 1 shows the accuracy values for existing and proposed methods. From the table it is clear that the proposed scenario yields higher accuracy values than the existing scenario.

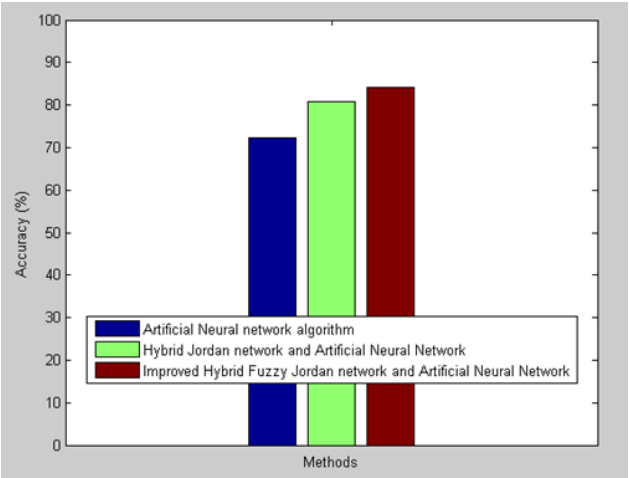

Figure 3. Accuracy

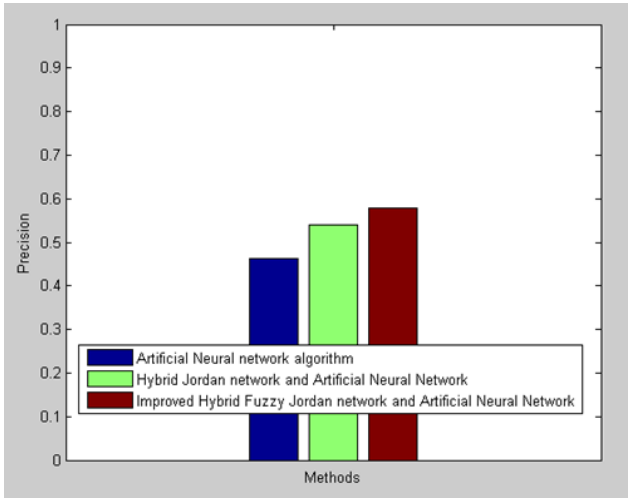

Figure 4. Precision

Table 1. Comparison values for the Intrusion

Parameters	Methods		
	ANN	HJANN	IHFJANN
Accuracy	72.26	80.90	84.12
Precision	0.46	0.54	0.57
Recall	0.73	0.80	0.84
F-Measure	0.56	0.64	0.68

Table 2. Comparison values for Convergence Iterations Detection System

S.No	Methods	Rate of Convergence
2	ANN	952
3	Hybrid Jordan ANN	899
4	Improved Hybrid Fuzzy Jordan ANN	764

5.2 Precision

Precision value is calculated based on the retrieval of information at true positive prediction, false positive. Precision is calculated as the percentage of positive results returned that are relevant.

$$\text{Precision} = \frac{\text{True positive}}{\text{True positive} + \text{False positive}}$$

From the Figure 4 it can be proved that the proposed methodology provides better result than the existing approach with better precision value. In this graph, the methods such as ANN, Hybrid Jordan network and ANN (HJANN) and Improved Hybrid Fuzzy Jordan ANN (IHFJANN) plotted in the x axis and the precision values are plotted in the y axis. The precision value is low by using the method of ANN and Hybrid Jordan network and ANN (HJANN). The precision value is increased significantly by using the proposed IHFJANN. From the experimental result we can conclude that proposed method is superior to existing system in terms of precision.

Table 2 shows the precision values for existing and proposed methods. From the table values it is clear that the proposed scenario yields better precision values than existing scenario.

5.3 Recall

Recall value is calculated based on the retrieval of information at true positive prediction, false negative. Recall is the fraction of relevant instances that are retrieved.

$$\text{Recall} = \frac{\text{True positive}}{\text{True positive} + \text{False negative}}$$

From the Figure 4 it can be proved that the proposed methodology provides better result than the existing approach with better recall value. In this graph, the methods such as ANN, Hybrid Jordan network and ANN (HJANN) and Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (IHFJANN) plotted in the x axis and the recall values are plotted in the y axis. The recall value is low by using the method of ANN and Hybrid Jordan network and ANN (HJANN). The recall value is increased significantly by using the proposed IHFJANN. From the experimental result we can conclude

that proposed method is superior to existing system in terms of recall.

Table 3 shows the recall values for existing and proposed methods. From the table values it is clear that the proposed scenario yields better recall values than existing scenario.

5.4 F-measure comparison

F-measure distinguishes the correct classification within different classes. It is a measure of a test's accuracy. It considers both the precision and recall test to compute the score. The F Measure score can be interpreted as a weighted average of the precision and recall, where an F_1 score reaches its best value at 1 and worst score at 0. It is defined as follows:

$$F-Measure = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

From the Figure 6 it can be proved that the proposed methodology provides better result than the existing approach with better F-measure value. In this graph, the methods such as ANN, Hybrid Jordan network and ANN (HJANN) and Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (IHFJANN) plotted in the x axis and the F-measure values are plotted in the y axis. The F-measure value is low when using the method of ANN and Hybrid Jordan network and ANN (HJANN). The F-measure value is increased significantly by using the proposed IHFJANN. From the experimental result we can conclude that proposed method is superior to existing system in terms of F-measure.

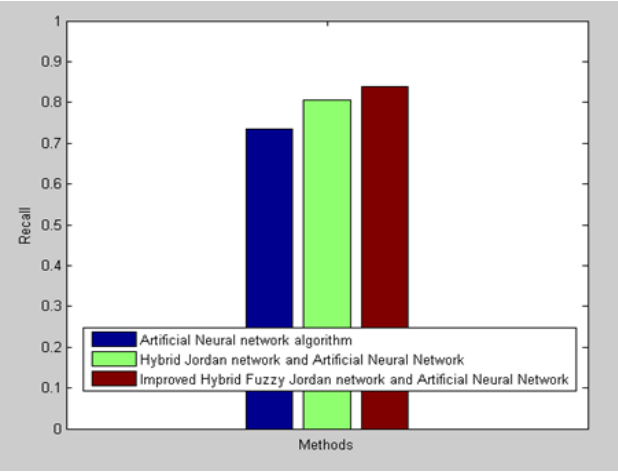

Figure 5. Recall

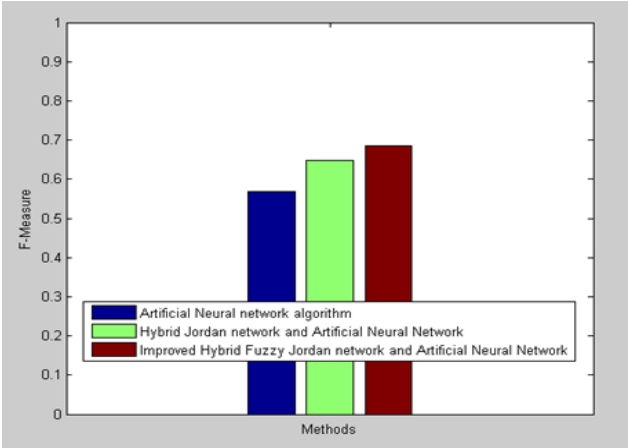

Figure 6. F-measure

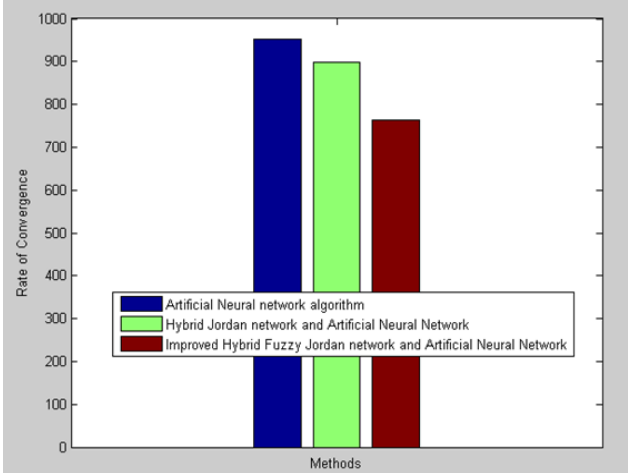

Figure 7. Rate of convergence

Table 4 shows the F-measure values for existing and proposed methods. From the table it is clear that the proposed scenario yields higher F-measure values than the existing scenario.

5.5 Convergence Iterations

From the Figure 7 it can be proved that the proposed methodology provides better result than the existing approach with reduced convergence rate. In this graph, the methods such as ANN, Hybrid Jordan network and ANN (HJANN) and Improved Hybrid Fuzzy Jordan network and ANN (IHFJANN) plotted in the x axis and the F-measure values are plotted in the y axis. The convergence iterations are high by using the method of ANN and Hybrid Jordan network and ANN (HJANN). The convergence iterations are reduced significantly by

using the proposed IHFJANN. From the experimental result we can conclude that proposed method is superior to existing system in terms of convergence iterations.

Table 5 shows the rate of convergence values for existing and proposed methods. From the table values it is clear that the proposed scenario provides minimum rate of convergence values than existing scenario.

6. Conclusion

The proposed Improved Hybrid Fuzzy Jordan network and ANN (IHFJANN) method increases the accuracy of prediction result in the intrusion detection system. This research scenario is used to analyze and discover the intrusions prominently by using the effective approaches. The convergence iterations are decreased significantly and the performance of the system is improved in the proposed technique. In future work, the neural dynamic system can also be used to observe the dynamic behaviour from the neural system and also it can be reduce the complexity of neural network by using advanced methods.

7. References

1. Revathi S, Malathi A. Intrusion detection based on fuzzy logic approach using simplified swarm optimization. 2014; 13(1):19–22.
2. Mehdi M, Anou ZA, Bensebti M. A bayesian networks in intrusion detection systems, in proc Journal of computer Science. 2007; 3(5):259–65.
3. Li W. Using genetic algorithm for network intrusion detection, in proceedings of the United States Department of Energy Cyber Security Group; 2004. p. 1–8.
4. Ahmad I, Abdullah AB, Alghamdi AS. Application of artificial neural network in detection of probing attacks. Proc IEEE Symposium on Industrial Electronics & Applications. 2009; 4(6):557–62.
5. Kriesel D, A brief introduction to neural networks. Available from: http://www.dkriesel.com/_media/science/neuronale-netze-en-zeta2-2col-dkrieselcom
6. Wang G, Hao J, Ma J, Huang L. A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Proc Expert Systems with Applications. 2010; 37(9):6225–32.
7. Mabu S, Chen C, Lu N, Shimada K,Hirasawa K. An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming. Proc IEEE Transactions. 2011; 41(1):130–9.
8. Mozelli LA, Souza FO, Palhares RM. New Lyapunov function and extra information on membership functions for improving stability conditions of TS systems. Proc IFAC World Congress. 2011; 28(2):3398–402
9. Srinivasu P, Avadhani. Genetic algorithm based weight extraction algorithm for artificial neural network classifier in intrusion detection. Proc Procedia Engineering, 2012; 38(1):144–53.
10. Mukherjee, Saurabh, Sharma N. Intrusion detection using naive Bayes classifier with feature reduction. Proc Procedia Technology. 2012; 2 (4):119–28.
11. Ganapathy S, Kulothungan P, Yogesh, Kannan A. A novel weighted fuzzy c-means clustering based on immune genetic algorithm for intrusion detection. Proc Procedia Engineering. 2012; 38(2):1750–7.
12. Elbasiony RM, Sallam EA, Eltobely TE. A hybrid network intrusion detection framework based on random forests and weighted k-means. Proc Ain Shams Engineering Journal. 2013; 4(4):753–62.
13. Wafa A. Applying artificial neural network and extended classifier system for network intrusion detection. Proc the International Arab Journal of Information Technology. 2013; 10(3):230–8.
14. Bhuyan MH, Bhattacharyya DK, Kalita JK. Network anomaly detection: methods, systems and tools, Communications Surveys & Tutorials. Proc IEEE Communications Surveys And Tutorials. 2014; 16(1):303–36.
15. Zebardast, Behnam, Maleki I, Maroufi A. A Novel Multilayer Perceptron Artificial Neural Network based Recognition for Kurdish Manuscript. Indian Journal of Science and Technology. 2014; 7(3):343–51.
16. Gharehchopogh, Farhad Soleimanian. A Novel PSO based Approach with Hybrid of Fuzzy C-Means and Learning Automata in Software Cost Estimation. Indian Journal of Science and Technology. 2014; 7(6): 795–803.