VOL. 11, NO. 13, JULY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

WEIGHT OPTIMIZED DYNAMIC HYBRID FUZZY JORDAN ARTIFICIAL NEURAL NETWORK FOR INTRUSION DETECTION

A. Dhivya[1] and S. N. Sivanandam[2]
[1]Karpagam University, Department of Computer Science, Coimbatore, India
[2]Emeritus, Karpagam University, Department of Computer Science, Coimbatore, India
E-Mail: adhivya123research@gmail.com

ABSTRACT

A Dynamic Hybrid Fuzzy Jordan Artificial Neural Network finds the intrusion very efficiently in timely behaviour varied networks. The development of DHFJAN is to influence the behavior of dynamic systems to achieve the pre-determinate objectives. In DHFJAN, the number of hidden layer in neural and Jordan networks and number of nodes in each hidden layers are determined at runtime based on error obtained in the training stage. Generally neural network and Jordan network approaches are inherent nonlinear optimization problem, the quality of Hybrid network local solution is determined the weight initialization. Stability and weight convergence are important issues in the performance analysis of dynamic networks. The weight initialization and optimization of hybrid networks is not discussed in DHFJAN. This paper finds the optimal weight values of each layer by utilizing the optimization techniques to improve the performance and final representation of hybrid network. Many researches were focused on the weight optimization of neural network using various optimization algorithm the PSO is best among them. Since two networks available in hybrid network, applying PSO leads time consumption because the search space size of PSO. This paper proposes a modified PSO algorithm named as CCPSO with constrained search space and controlled convergence degree. The constrained search space is achieved by generating initial weight values based on power-law distribution and Zipf's law. Convergence degree of population in the PSO is controlled by analyzing mean and variance values of fitness in each iteration. The optimal weights are updated in hybrid dynamic network while neuron state changing. Thus the proposed approach improves the performance of dynamic hybrid fuzzy Jordan neural network and also reduces the error rate significantly. Experimental result shows that the proposed WDHFJANN is better than the DIHFJANN.

Keywords: Jordan network, particle swarm optimization (PSO), intrusion detection, artificial neural network (ANN), convergence.

1. INTRODUCTION

An intrusion detection mechanism is an important application utilized for monitoring the system and defending it from an intruder. With the rapid growth in the internet based expertise new application fields for computer system have emerged. For instances, the areas such as commerce, economy, industry, security and healthcare sectors requires security due to big vulnerability issues. Malicious users utilize the association's interior networks to gather data's and cause vulnerabilities such as bugs, errors, worms, virus and lapse in network. Intrusion detection system discovers unauthorized invasions into network computer resources [1]. The intrusion detection system observes network traffic of computer network such as a network sniffer and gathers network log records. It raises alarm while any rule violation is identified the intrusion detection system alerts the network admin [2].

There are two types of mechanisms like static and dynamic systems. The static methods are such as firewalls and software updates producing a practical security level and dynamic systems are used to observe the random behavior of system efficiently. The intrusion discovery system depends on either network based or host based attacks. The network based attacks are mainly based on misuse or anomaly based attacks. The network based attacks are detected from the interconnection of computer systems. Since the system communicates with each other, the attack is sent from one computer system to another computer system by the way of routers and switches. These attacks mostly take place from some outside devices which are associated. The web based intruders are possible while networks are linked over the internet and the intrusions can be extended into diverse networks via the electronic message, discussion, downloading the materials etc. Currently numerous computer systems are affected from web based hazardous attacks [3].

To effectively handle the intrusions, the machine learning approaches and optimization algorithms are introduced in the intrusion detection system. The machine learning approaches are classified into two types such as Artificial Intelligence (AI) method and Computational Intelligence (CI) method. AI method refers to the approaches from the area of statistical modeling and CI method refers to nature inspired approaches which are utilized to deal with difficult issues [4]. Several machine learning methods are suggested to discover the intrusions behavior for progress the detection rates significantly. The AI based methods includes supervised and unsupervised algorithms to identify the intrusions in the specified system. The supervised algorithms are such as decision tree, K Nearest Neighbor (KNN) And Support Vector Machine (SVM). The unsupervised algorithms are such as k means clustering and single linkage clustering. The CI based methods includes genetic algorithm, artificial neural network and fuzzy logic algorithms to detect optimal solutions.

The fuzzy based intrusion system provides major advantages in the field of intrusion detection applications

[5]. The fuzzy class association rule mining based on genetic algorithm is able to detect the mixed type of attributes and also eliminate the sharp boundary issue [6]. Genetic approach is utilized to extract several rules which are needed for anomaly discovery mechanisms. Association rule mining approach is use to mine adequate number of prominent rules for the user's purpose rather than to mine all rules meeting the constraints which are very helpful for misuse detection [7] [8]. Fuzzy genetic algorithm is importantly useful for testing the knowledge discover in database (KDD'99) intrusion dataset more effectively. The hybrid fuzzy logic and neural network are also introduced to deal with intrusions as well as recognize attacks significantly in the computer networks.

2. LITERATURE REVIEW

In [9], Reyadh Shaker Naoun *et al* suggested back propagation artificial neural network for intrusion detection systems. This research scenario is able to deal with large number of attacks and potentially found by enhanced approach. In this scenario, a multilayer perceptron is skilled with the help of improved resilient back propagation training approach. It is used to enhance the convergence speed with optimal and ultimate learning factor which are added to the weight update function. The suggested approaches are able to identify the false positive rates by using supervised learning and unsupervised learning approaches. This research scenario is used to improve the precision, recall and accuracy values. In [10], Hatim Mohamad Tahir *et al* suggested hybrid machine learning technique for intrusion detection. This scenario enhanced a hybrid machine learning system for network invasion discovery depends on mixture of K-means clustering and support vector machine classification algorithm. The plan of this work is to lessen the error rates by means of false positive as well as false negative and to improve the recognition rate.

In [11], Qing Song *et al* discussed robust initialization of a Jordan network along with recurrent constrained learning. To handle the issue of training and testing errors, this research scenario has introduced an efficient approach named as a robust initialization of a Jordan network with recurrent constrained learning algorithm. It is designed for multilayered recurrent neural network. The main aim of this approach is solving the issues of weight initialization and selection of the hidden layer neurons through a novel recurrent sensitivity ratio analysis. In [12], Xiaoyu Wang *et al* suggested convergence study in extended Kalman filter based training of recurrent neural network. This research scenario is focused on the improving an efficient approach to speed up the convergence rate. In this scenario, the methods are utilized the two parameters such as covariance of measurement noise and covariance of process noise. Hence these artificial training noise parameters are useful to stabilize the recurrent neural network and accelerate the training process.

In [13], Jing-Ru Zhang *et al* recommended a hybrid particle swarm optimization algorithm with back propagation for forward neural network training. To improve the weight initialization and optimization concept, the hybrid approach is introduced in this scenario. The hybrid algorithm is used to reduce the wasting too much searching time and progress the searching efficiency. In [14], Hong-Wei Ge *et al* discussed an improved particle swarm optimization based dynamic recurrent neural network for identifying and controlling non linear systems. This research scenario is focused on the robust performance of network and optimized weight selection. It reduces the time complexity as well as space complexity significantly and improves the convergence speed.

In [15], Dharmistha *et al* discussed about genetic algorithm based weight optimization of artificial neural network. This approach is used to select the optimal weights and make the network more reliable. It is also used to determine the stopping point before over fitting occurs. A typical fitting criterion may be introduced to emphasize the model validity. Such criterion may be mean square error (MSE), sum square error (SSE) which is calculated between the target and the network output.

3. MATERIALS AND METHODS

Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network (DHFJANN)

In the preceding research, the dynamic hybrid fuzzy Jordan artificial neural network is introduced to discover the number of hidden layer in neural and Jordan network. This research is also used to determine the number of nodes in every hidden layer. In this scenario, the method is focused on the discovering the dynamic intruders in the specified neural network. It avoids the error rate significantly and overcomes the issues which are occurred in the static networks. The training time is faster and their parameters are changed in certain time interval.

Behavior based intrusion discover methods are identified the deviation from normal or expected behavior of the users. The reference information is like timestamps and payload size is used to model the normal or valid behavior. It is gathered through various means which can be included along with other feature to progress the accuracy of fuzzy Jordan artificial neural network. To increase the speed of the convergence rate, the research scenario is introduced modified steepest gradient algorithm. It is used to reduce the error rate more effectively and optimize the number of hidden nodes by using complexity regularization. The first order and second order are such as mean, variance, Skewness and Kurtosis, time varying moment, correlation computed. It provides better detection of intrusion results but it does not consider the weight initialization and optimization in the dynamic networks.

Proposed Methodology

Weight optimized Dynamic Hybrid Fuzzy Jordan Artificial Neural Network

In this section, to improve the stability and weight convergence, this research scenario is enhanced the technique named as weight optimized dynamic hybrid Jordan artificial neural network. To achieve the weight optimization concept, this scenario has introduced the optimization algorithm called as particle swarm optimization (PSO). The optimization approach is used to calculate the optimal weight values of each layer which is used to increase the hybrid network performance. The PSO algorithm is used to estimate the weight optimization concept on both the Jordan network and neural network. The main motivation of the optimization algorithm is reducing the searching space complexity and computational time complexity in the hybrid network significantly.

In this research scenario, the proposed PSO algorithm is based on the learning concept of neural network and Jordan network along with weight optimization value. The algorithm considers the optimal parameters such as minimum search space, optimized weight value and optimal neurons. To ensure this objective function, the PSO algorithm is modified along with constrained search apace and controlled convergence degree. Thus the proposed algorithm is named as CCPSO and the objective function of CCPSO is achieved in the weighted dynamic hybrid fuzzy Jordan neural network. The DHFJANN obtains faster convergence rate and also leads more robustness of the network.

The initial weight values are generated based on the power law distribution and zipf's law. The power law is a functional relationship between two quantities or particle weights where a relative change in one quantity results in a proportional comparative variation in other measure, independent of the initial size of those measures. The power law is defined as given below:

$$f(cx) = a(cx)^{-k} = c^{-k} f(x) \propto f(x) \quad (1)$$

Where, scaling the argument x by a constant factor c and power law constant is c^{-k} and scaling function is f.

Zipf's law is defined as the prediction of frequency elements which is occurred in terms of rank order and reciprocal rank order.

The zipf's law is defined as given below:

$$f(k, s, N) = \frac{1/k^s}{\sum_{n=1}^{N} 1/n^s} \quad (2)$$

Where, N is the number of elements, k is their rank, s is the value of the exponent characterizing the distribution.

Weight initialization is the most important factor to increase the speed up of training of neural network. The controlled convergence degree is used to discover the optimal initial weights. Through the statistical analysis, the maximum weight values are obtained in this network. Hence this proposed research is used to detect the high number of intrusions in the dynamic hybrid network more effectively rather than the previous research.

Weight optimization is improved by CCPSO algorithm in the hybrid network which is reducing the space complexity and time complexity significantly. The algorithm is detecting the optimal weights and such kinds of weights are updated in the dynamic hybrid fuzzy Jordan and artificial neural network when neuron state changing.

$$v_{id}^{k+1} = wv_{id}^{k} + c_1 r_1 (p_{id} - x_{id}^{k}) + c_2 r_2 (p_{gd} - x_{id}^{k}) \quad (3)$$

$$x_{id}^{k+1} = x_{id}^{k} + v_{id}^{k+1} \quad (4)$$

Where $X_i = (x_{i1}, x_{i2}, \ldots, x_{iD})$ is the position of the i-th particle in D-dimension, $V_i = (v_{i1}, v_{i2}, \ldots, v_{iD})$ is its velocity which represents its direction of searching.

In which i=1, 2,……N, N-th population of the group particles, d=1, 2,….D, k-the maximum number of iteration, r_1, r_2-random values between [0,1], c_1, c_2-learning coefficients

v_{id}^{k}-the number of d component of the velocity of the particle I in the k-th iterating

x_{id}^{k}-the number d component of the position of particle i in k-th iterating

p_{id}-the number d component of the best position particle i has ever found

p_{gd}-the number d component of the best position the group particles have ever found.

Algorithm 1

CCPSO algorithm

1. Initialize the position and velocity of each particle
2. Compute the fitness of each particle
3. Concern the particle along with the biggest fitness value, reinitialize its position.
4. Evaluate the particle along with the smallest fitness value whether its new position is acceptable
5. Update its position or else new position is assigned to the particle using (3) and (4)
6. For each particle, compare its current fitness value with the fitness of its pbest, if the current value is better, and then update pbest and its fitness value;
7. Determine the best particle of group with the best fitness value, if the current fitness value is better than the fitness value of gbest, then update the gbest and its fitness value with the position;
8. Check the finalizing criterion, if it has been satisfied, quit the iteration; otherwise, return to step 3).

DHFJANN mechanism with CCPSO algorithm

The neural network input vector is given below:

$$x(k)=[u^T(k)\ y^T(k-d)\ \ldots\ y^T(k-d)]^T \in R^{n\times 1} \quad (5)$$

The output of neural network can be represented by

$$y(k) = V(k)\Phi(W(k), x(k)) \quad (6)$$

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

Where n = p+h×d-dimensional vector in which d is the maximum time delay factor.

The errors or intrusions reduced by the fuzzy function

$$e=diff(Y,D)=\frac{1}{2}\sum[(y_1^{(k)}-d_1^{(k)}]^2+(y_2^{(k)}-d_2^{(k)})^2 \quad (8)$$

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

Objective function

Achieve error minimization function

$$E_k=\sum_{i=1}^{q}(y_i^k-C_i^k)^2 \quad (9)$$

$$E=\sum_{k=1}^{q}E_k/(q*q) \quad (10)$$

Algorithm 2

1. Initialize the input parameters in the dynamic hybrid network
2. Initialize the position and velocity of each particle p1, p2….pn // each particle represents individual network structure
3. Compute objective function using (10)
4. Compute the hidden nodes with position values
5. Find out the current best particle among all particles
6. Update current best particle with its velocity
7. Compute for each particle with the current best particle and compare the current fitness value in the hybrid network
8. If previous particle is best then compute all particles towards the best particle
9. Choose the current best particle and update the current best particle's position and velocity
10. Reduce the error rate and increase the accuracy value

Algorithm procedure

1. Start with number of hidden layer fuzzy neurons.
2. Selection is based on the previous knowledge of the neurons.
3. Set a maximum weight-initialization step.
4. Initialize the dynamic Jordan and neural with the associated random weight initialization using (1) and (3)
5. Update the recurrent input vector x(k) in (5)
6. Compute the neural network output *y(k)* and real time estimate error by using (6) and (7) respectively.
7. Apply the algorithm 2
8. Discover the initial weight values using (1) and (2)
9. Algorithm 1 generates the optimal weight using fitness function
10. Go to step 4 and continue until the end of the training data points
11. Save the values for particular weight initialization step for the iterative training and continue until the maximum weight-initialization number is reached.
12. Obtain the resultant weight initialization as the most excellent value for the training based on the chosen number of hidden layer fuzzy neurons.
13. Optimized weights are updated
14. Convergence speed is increased.

The statistical analysis is utilized such as mean and variance to analyze the convergence degree of population in particle swarm optimization algorithm. It is used to improve the detection accuracy in terms of reduction in error rate on the hybrid dynamic network.

4. RESULTS AND DISCUSSIONS

In this section the performance metrics are compared among the existing and proposed scenarios by using efficient methodologies. Back propagation neural network algorithm is an important technique to classify the intrusion detection. Radial Basis Function (RBF) and every neuron include the RBF on a point with several features. RBF network contains two layers such as hidden and output layer. Input is mapped into every RBF in the hidden layer and RBF is used to progress the speed of training data. The output has four class labels in the specified 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 are such as Denial of Attacks (DOS), probe, Remote to Local Attack (R2L) and User to Root Attack (U2R). The sub types of DOS are back DOS, land DOS, Neptune DOS, pod DOS, smurf DOS and teardrop DOS attacks. The sub types of R2L are ftp_write R2L, guess_passwd R2L, imap R2L, multihop R2L, phf R2L, spy R2L, warezclient R2L and warezmaster R2L. The sub types of U2R are buffer_overflow U2R, loadmodule U2R, perl U2R and rootkit U2R. The sub types of probe are ipsweep probe, nmap probe, portsweep probe and Satan probe. The training dataset includes 2500 tuples and 38 attributes whereas the testing dataset includes 995 tuples and 38 attributes.

The methods are analyzed and compared with the performance of neural networks for intrusion detection. Such kinds of methods are existing Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network (DIHFJANN) and proposed Weight optimized Dynamic Hybrid Fuzzy Jordan ANN (WDHFJANN). To increase the accuracy as well as efficiency, the dynamic parameters are utilized in this scenario. From the experimental result we can conclude that the proposed methodology is used to improve the prediction accuracy and also used to speed up the convergence rate significantly. Hence WDHFJANN is superior in the detection of intrusions dynamically and overall system performance.

Accuracy

The 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,

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

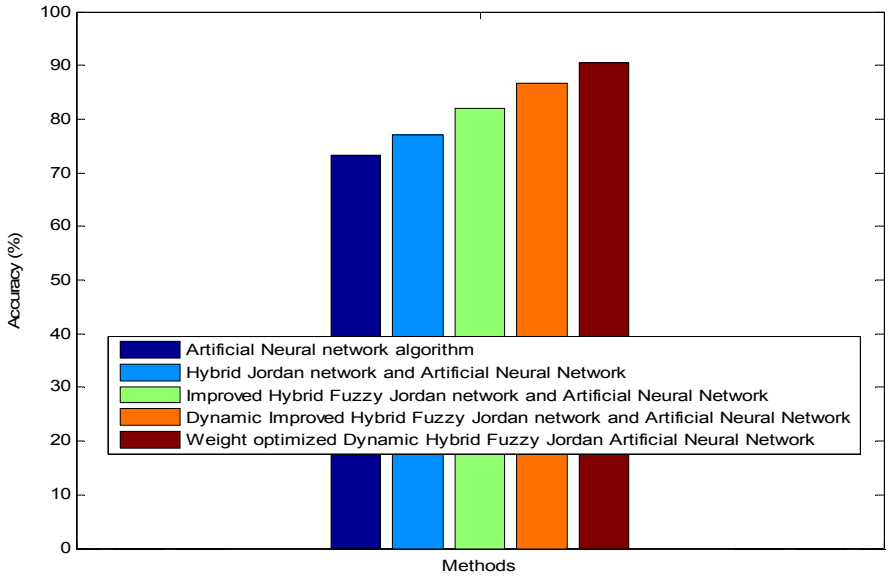


Figure-1. Accuracy comparison.

From the Figure-1 it can be proved that the proposed methodology provides better result than the existing approach by increasing the accuracy value. In this graph, the methods are such as ANN, HFJANN, IHFJANN, DIHFJANN and WDHFJANN plotted in the x axis and the accuracy values are plotted in the y axis. The accuracy value is low by using the existing method of ANN, HFJANN, IHFJANN and DIHFJANN. The accuracy value is increased significantly by using the proposed WDHFJANN. Thus, the proposed method is used to predict the intrusions efficiently. From the experimental result we can conclude that proposed method is superior to existing system.

Precision

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

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

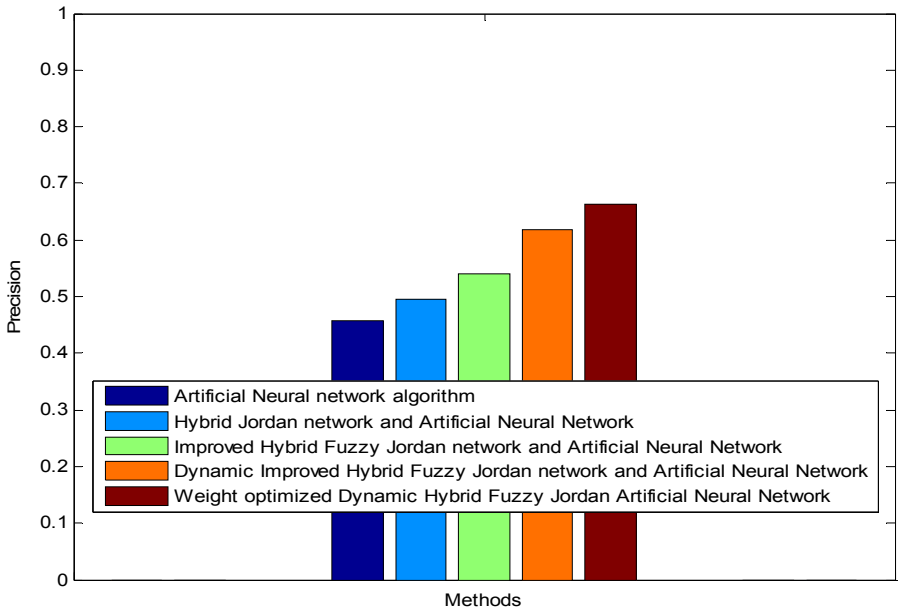


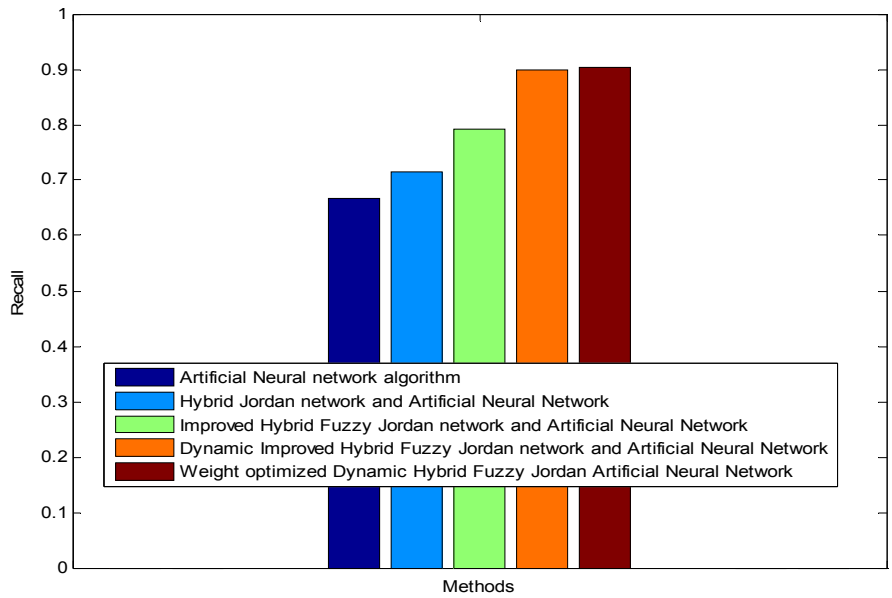
Figure-2. Precision comparison.

From the Figure-2 it can be proved that the proposed methodology provides better result than the existing approach by increasing the precision value. In this graph, the methods are such as ANN, HFJANN, IHFJANN, DIHFJANN and WDHFJANN plotted in the x axis and the precision values are plotted in the y axis. The precision value is low by using the existing method of ANN, HFJANN, IHFJANN and DIHFJANN. The precision value is increased significantly by using the proposed WDHFJANN. Thus, the proposed method is used to predict the intrusions efficiently. From the experimental result we can conclude that proposed method is superior to existing system.

Recall

Recall value is calculated based on the retrieval of information at true positive prediction, false negative. In healthcare data precision is calculated the percentage of positive results returned that are Recall in this context is also referred to as the True Positive Rate. Recall is the fraction of relevant instances that are retrieved,

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



Figuire-3. Recall comparison.

From the Figure-3 it can be proved that the proposed methodology provides better result than the existing approach by increasing the recall value. In this graph, the methods are such as ANN, HFJANN, IHFJANN, DIHFJANN and WDHFJANN plotted in the x axis and the recall values are plotted in the y axis. The recall value is low by using the existing method of ANN, HFJANN, IHFJANN and DIHFJANN. The recall value is increased significantly by using the proposed WDHFJANN. Thus, the proposed method is used to predict the intrusions efficiently. From the experimental result we can conclude that proposed method is superior to existing system.

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 the recall of the 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:

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

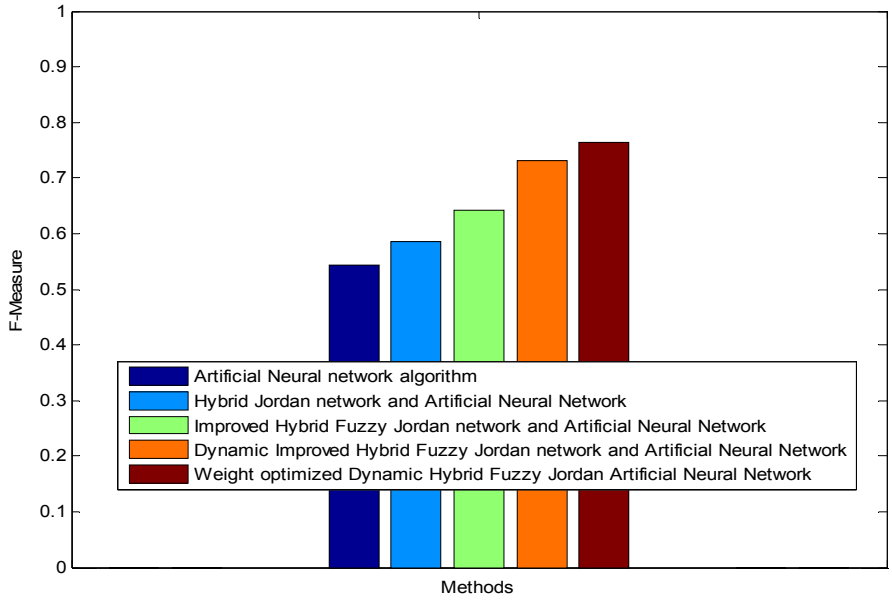


Figure-4. F-measure comparison.

From the Figure-4 it can be proved that the proposed methodology provides better result than the existing approach by increasing the F-measure value. In this graph, the methods are such as ANN, HFJANN, IHFJANN, DIHFJANN and WDHFJANN plotted in the x axis and the F-measure values are plotted in the y axis. The F-measure value is low by using the existing methods of ANN, HFJANN, IHFJANN and DIHFJANN. The F-measure value is increased significantly by using the proposed WDHFJANN. Thus, the proposed method is used to predict the intrusions efficiently. From the experimental result we can conclude that proposed method is superior to existing system.

Convergence iterations

From the Figure-5 it can be proved that the proposed methodology provides better result than the existing approach by speed up the convergence rate. In this graph, the methods are such as ANN, HFJANN, IHFJANN, DIHFJANN and WDHFJANN plotted in the x axis and convergence rate values are plotted in the y axis. The convergence speed is reduced by using the existing methods of ANN, HFJANN, IHFJANN and DIHFJANN. The convergence speed is increased significantly by using the proposed WDHFJANN. Hence, the proposed method is used to predict the intrusions efficiently. From the experimental result we can conclude that proposed method is superior to existing system.

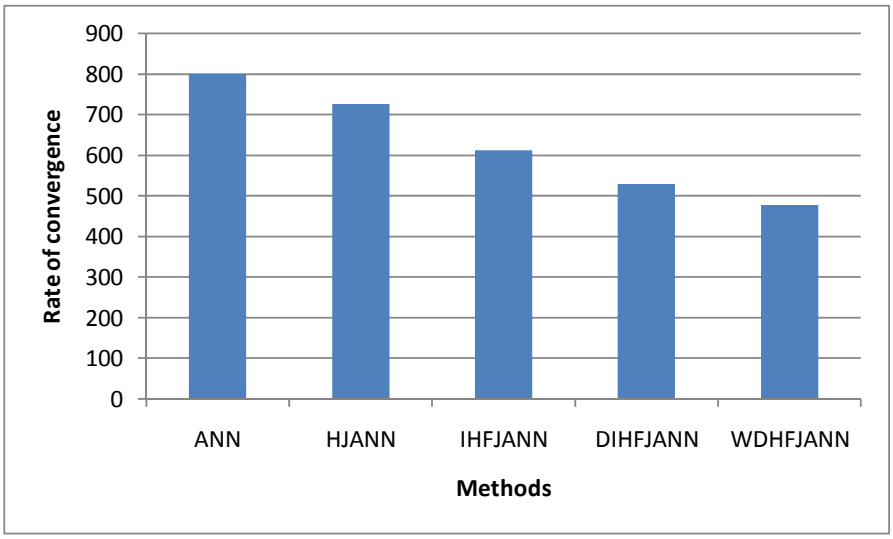


Figure-5. Rate of convergence.

Table-1. Comparison values for the Intrusion Detection System.

Parameters	Methods				
	ANN	**HFJANN**	**IHFJANN**	**DHFJANN**	**WDHFJANN**
Accuracy	73.26	77.08	82.01	86.61	90.45
Precision	0.45	0.49	0.53	0.61	0.66
Recall	0.68	0.71	0.79	0.89	0.90
F-measure	0.54	0.58	0.64	0.73	0.76

The Table-1 shows the different rate of convergence values for existing and proposed methods. The methods are ANN, HJANN, IHFJANN, DHFJANN and WDHFJANN approaches. WDHFJANN based intrusion detection system's accuracy, precision, recall also f-measure rate is higher than the ANN, HJANN, IHFJANN and DHFJANN approaches. From this experimentation, it is concluded that the WDHFJANN based intrusion detection system is effective and efficient rather than the preceding methods.

Table-2. Comparison values for the convergence iterations.

S. No.	Networks	Rate of Convergence
1	ANN	800
2	HJANN	726
3	IHFJANN	611
4	DIHFJANN	528
5	WDHFJANN	476

The Table-2 shows the different rate of convergence values for existing and proposed methods. The methods are ANN, HJANN, IHFJANN, DHFJANN and WDHFJANN approaches. The WDHFJANN based intrusion detection system has the high speed of convergence rate compared to the ANN, HJANN, IHFJANN and DHFJANN methods. From this experimentation, it is concluded that the WDHFJANN based intrusion detection system is effective and efficient rather than preceding method.

5. CONCLUSIONS

The proposed Weight optimized Dynamic Hybrid Fuzzy Jordan Artificial Neural Network (WDHFJANN) based method has improved the accuracy of prediction result in the intrusion detection system. This weight optimized hybrid dynamic network is used to select optimal weights and discover the intruders more efficiently using optimization algorithm. The space search complexity is reduced significantly and the error rate is reduced effectively rather than preceding research. The convergence speed is increased and the performance of the hybrid dynamic system is increased higher in the proposed technique. In future work, the new rules can be generated from the hybrid fuzzy network which can be focused to detect the numerous attacks. The future work can extend in terms of feature subset selection and it will be used to

improve the intrusion detection performance significantly by using advanced feature selection techniques.

REFERENCES

[1] Patel, Jaina and Mr Krunal Panchal. 2015. Effective Intrusion Detection System using Data Mining Technique. In JETIR. 2(6).

[2] Anyanwu Longy O. 2010. Dynamically Self-adapting and Growing Intrusion Detection System. In International Journal of Multimedia and Ubiquitous Engineering. 5(3).

[3] Devaraju S. and S. Ramakrishnan. 2014. Performance comparison for intrusion detection system using neural network with KDD dataset. ICTACT Journal on Soft Computing. l 4.3.

[4] Zamani Mahdi. 2013. Machine Learning Techniques for Intrusion Detection, arXiv preprint arXiv: 1312.2177.

[5] Chaudhary Alka. 2014. Neuro-fuzzy based intrusion detection systems for network security. Journal of global research in computer science. 5(1): 1-2.

[6] Danane Yogita and Thaksen Parvat. 2015. Intrusion detection system using fuzzy genetic algorithm. Pervasive Computing (ICPC), 2015 International Conference on. IEEE.

[7] Dhopte Swati and N. Z. Tarapore. 2012. Design of Intrusion Detection System using Fuzzy Class-Association Rule Mining based on Genetic Algorithm. International Journal of Computer Applications (0975-8887) Vol. (2012).

[8] Jawhar Muna Mhammad T. and Monica Mehrotra. 2010. Design network intrusion detection system using hybrid fuzzy-neural network. International Journal of Computer Science and Security. 4(3): 285-294.

[9] Naoum Reyadh Shaker, Namh Abdula Abid and Zainab Namh Al-Sultani. 2012. An Enhanced Resilient Backpropagation Artificial Neural Network for Intrusion Detection System, International Journal of Computer Science and Network Security. 12(3): 11-16.

[10] Hasan Wael and Mohd Hasbullah Omar. 2015. Hybrid machine learning technique for intrusion detection system, In: 5th International Conference on Computing and Informatics, ICOCI.

[11] Song, Qing. 2010. On the weight convergence of Elman networks, Neural Networks, IEEE Transactions on. 21(3): 463-480.

[12] Wang Xiaoyu and Yong Huang. 2011. Convergence study in extended Kalman Filter-based training of recurrent neural networks, Neural Networks. IEEE Transactions on. 22(4): 588-600.

[13] Zhang Jing-Ru, et al. 2007. A hybrid particle swarm optimization-back-propagation algorithm for feed forward neural network training, Applied Mathematics and Computation. 185(2): 1026-1037.

[14] http://www.science.unitn.it/~marchese/pdf/CS%2020060413.pdf.

[15] Ms. Dharmistha and D. Vishwakarma. 2012. Genetic Algorithm based Weights Optimization of Artificial Neural Network. In International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. 1(3).