DYNAMIC IMPROVED HYBRID FUZZY JORDAN NETWORK FOR ROBUST AND EFFICIENT INTRUSION DETECTION SYSTEM

Dhivya . A[1], Sivanandam . S[2]

ABSTRACT

The security is an important aspect to protect the information systems and networks against attacks. Intrusion Detection System assists information systems practice to deal with attacks. A hybrid fuzzy Jordan artificial neural network was proposed to detect intrusion based on learned model. However fuzzy Jordan artificial network is static which cannot handle the dynamic behavior of intruder, the behavior-based intrusion detection techniques detects intrusion by observing a deviation from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information such as timestamps, sizes of the payloads, and TCP-flags of all packets etc and is collected by various means which can be incorporated with other static feature to improve the accuracy of hybrid fuzzy Jordan artificial neural network. The time varying features are extracted from captured packet information with sliced time window. The first order statistics Variance, Skewness and Kurtosis, second order statistics correlation, entropy and moment of time varying features are calculated to use in the classification along with actual value of this features to improve the prediction accuracy. The network structure of hybrid fuzzy Jordan artificial neural network is decided dynamically based on the error achieved while learning stage. Although somewhat more difficult to train, Dynamic networks are generally more powerful than static networks, because dynamic networks are trained to learn sequential or time-varying patterns. The intruder's parameters are not static; their parameters are varied at certain time interval. In this paper Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network (DIHFJANN) is proposed to handle dynamic behavior intruders. The Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network utilize modified steepest-gradient algorithm which solves the relatively slow and inferior of asymptotic rate of convergence problems of steepest gradient algorithm. In modified steepest gradient algorithm original global minimization problem is transformed into a quadratic-form minimization based on the steepest descent method and the current iterative point. The structure of Hybrid Fuzzy Jordan Artificial Neural Network such as number of hidden layer and the number of node in the hidden layer is dynamically adjusted based on the error value obtained in the training stage using complexity regularization approach. The experimental result shows the reduction of time complexity and performance up gradation using DIHFJANN method.

I. INTRODUCTION

The rapid growing of computer networks and interconnection between them has been prone to some security issues. Intrusion detection system is a significant aspect as very huge degree of perceptive information is stored and processed in network systems across the world. The main aim of intrusion detection system is to discover the number of attacks against information systems effectively [1]. The intrusion detection system is widely

[1]Research Scholar, Karpagam University. CSE. Coimbatore, India.

[2]Professor Emeritus, CSE - KCE

divided into two categories such as signature based and anomaly based systems. Signature detection is also named as misuse detection which is generally focused on the uncovering of known patterns of unauthorized users. The anomaly based systems are used to discover the abnormal and normal behavior patterns. Afterwards, if any activity deviates from the normal instance, then it is considered as intrusion [2]. Anomaly detection technique possesses the capability to discover the previous unknown attacks and hence it is more efficient rather than the signature based.

Krishna Kant Tiwari [3] et.al suggested data mining methods to deal with the huge intrusions in the given system. The methods are such as Artificial Neural Network (ANN) and Support Vector Machine (SVM) to detect the attacks using training process and specified model. Classification concept is used to increase the detection rate. It is also robust in case of known attacks. Association methods are focused on the analysis of similar instances occurred frequently and it detects the outliers more effectively. In Mabu, Shingo, et al [4], an efficient machine learning approaches are recommended for discovering network intrusions in high dimensional data. By merging fuzzy set theory along with genetic network programming, it can handle the mixed database such as discrete and continuous attributes. It is used to mine several significant class association rules that improve the detection ability.

In Benamara et al [5] the static networks are utilized that are difficult to train as it requires extensive training sets of system event records in order to differentiate normal behavior patterns. In this research, the networks are improved which is used to discover the dynamic characteristic of intruders. The dynamic networks have the potential to examine the time interval models. An Elman network [6] is applied to train the neural network with discrete time sequence predictions. The weight convergence is computed and improves the performance of Elman network based on the Lyapunov function. Thus the fully adaptive learning technique is utilized to optimize convergence speed which maximized the training as well as testing performances.

Jordan neural network [7] is introduced to discover the sql based attacks more efficiently and it is also similar structure of Elman network. Recurrent neural network is a dynamic network which has internal state in each time step of classification. This is due to circular links among higher and lower layer neurons and self feedback connections. Such type of connections activates recurrent neural networks to propagate data from previous events to current processing steps. Hence, this neural network constructs a memory of time series events. The dynamic fuzzy Jordan neural network is more suitable for intrusion detection network in specific time interval.

The remainder of the paper is summarized as: section II explains the related researches briefly. Section III presents the methodologies utilized in the paper. Section IV provides the experimental results and their discussions. Section V concludes the research.

II. Related works

Peter Tino et.al [8] recommended recurrent neural network along with small weights and memory models. This research scenario has proved the uniformity among issues handled by recurrent network. In this research, the behavior of instances is discovered efficiently and the

training process is improved. However this scenario failed to observe the random behavior from networks. Robert Koch et.al [9] suggested behavior based intrusion detection in encrypted environments. Preceding researches are failed to deal with privacy concepts in intrusion detection networks. To avoid this particular issue, this research presented a new behavior based detection mechanisms which is used to identify the intrusions as well as insider behaviors. Thus, the methods achieved the higher number of detection rates in the encrypted environment with better privacy levels. Since it used certain parameters to preset the architecture, optimization of those values is essential which is not included in this research.

Ahmed Youssef et.al [10] discussed network intrusion detection by using data mining approaches and network behavior analysis. In this research, potential malicious behaviors are found in the network traffics. It improves the detection of malicious activities based on the construction of network model behaviors. It also discovers the new patterns which prominently deviate from the normal network behavior. And also it is not yet introduced into the real world intrusion systems. M.Z.Rehman et.al [11] presented gradient descent back propagation algorithm that focused on the classification problems to progress the accuracy. In this research, algorithm had improved the previous working performance of back propagation by adaptively changing the momentum value as well as maintaining the gain parameter fixed for all nodes in the given network. This research speeded up the convergence rate than any other methods.

Rick Hofstede et.al [12] discussed real time intrusion detection for netflow and ip fix. This research scenario was focused on the functional extension for NetFlow and IPFIX flow exporters, to permit for timely intrusion discovery which reduces the huge number of attacks. It incorporated a lightweight intrusion discovery nodule to flow exporter which moved discovery closer to the traffic inspection point. Also this research reduced the attacks through learning firewalls to eliminate malicious traffic. And it prevents the given system from the overhead issues more effectively. The bottleneck of a system was found when the load increases, since the scripts are processed using generic CPU. Wei Wu et.al [13] suggested convergence of gradient technique along with momentum for back propagation neural network. This research was used to avoid the issues of gradient of the error function and slow convergence. The main aim of this research involved the hidden layer along with weight optimized values and the output layers of the back propagation network was consistently bounded. To achieve this objective, this work was considered the gradient technique with momentum for back propagation neural network. The momentum coefficient was selected in an adaptive way to speed up and stabilize the learning process of the network weights.

Chein-Shan Liu [14] discussed about the modifications of steepest descent technique and conjugate gradient method against noise in the network. In this research, the modified conjugate gradient approach which played an important role to improve the efficiency, accuracy and computational complexity issues. It is also significantly robustness against the noise for high dimensional data and increases the system performance. In [15], Alka

Chaudhary et.al suggested neuro-fuzzy based intrusion detection system for network security. This research mainly focused on the minimization of possible attacks in the given network. The fuzzy based intrusion technique was utilized to discover the attack rates efficiently. The fuzzy logic generates the rules depending on the information data and about the traffic patterns and it also protects the system from attacks. It also had better performance in terms of reduction in error rate and higher security.

III. Methodologies

Hybrid Fuzzy Jordan network and Artificial Neural Network (HFJANN)

This system adapts the fuzzy concept for the discovery of intrusion in the neural networks. The hybrid of Fuzzy System and Neural Network is used for more accurate prediction and also to increase the speed of the network. Fuzzy optimal control method predicts the intrusions by using Neural Network algorithm effectively and rapidly. Hence this concept maximizes more accurate decision in the neural network applications. However this scenario is used only in static network and it does not handle the dynamic behavior of the intruders.

Dynamic Improved Hybrid Fuzzy Jordan network and Artificial Neural Network (DIHFJANN)

To observe the dynamic behavior of the intruders of the system, the dynamic hybrid fuzzy Jordan ANN is introduced. This research is based on the behavior of the Neural Network which is used to detect the dynamic intruders more effectively. DIHFJANN is used to reduce the error rate significantly and also it takes minimum time for execution. A new algorithm is introduced named as Modified Steepest Gradient Algorithm which is used to improve the speed of the convergence rate in this network. DIHFJANN regulates the number of hidden layer and number of nodes in hidden layer using complexity regularization approach.

In this research, as the parameters of the network and the behavior of the intruders changes with respect to time, behavior based intrusion detection system is used discover the activities of abnormal intruders of the network. It is focused on monitoring the network traffic, event threats and node movements which is used to detect the abnormal behaviors dynamically. The intruder behavior changes due to actions not happened for a certain interval of time. Thus, the proposed DIHFJANN method is able to deal with dynamically varying behavior of intruder based on the modified steepest-gradient algorithm. This algorithm is used to solve the time-varying optimization problems.

Algorithm 1

Modified steepest-gradient algorithm

Given an initial x_0, $d_0 = -g_0$ and a convergence tolerance tol

For k=0 to max do

Set $\alpha_k = \text{argmin}\ \phi(\alpha)$

$x_{k+1} = x_k - \eta \frac{\|g_k\|^2}{g_k^T A_k g_k} g_k$ // where $\eta = 1 - \gamma$

Compute $g_{k+1} = \nabla f(x_{k+1})$

If $\|g_{k+1}\|_2 \leq tol$ then

Converged

End if

End for

Formula description

The neural network input is given below

$$H_{iN}(k) = W_{iN}(k)x(k) \quad (2)$$

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

The output of neural network can be represented by

$$y(k) = V(k)\Phi(W(k), x(k)) \quad (2)$$

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

Jordan network input is given below

$$H_{ij}(k) = W_{ij}(k)x(k) + c(k) \quad (3)$$

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

$$e(k) = [e_1(k) \ldots\ldots e_h(k)]^T \quad (4)$$

Where e (k) is error minimization function

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

$$e=\text{diff}(Y,D)=\frac{1}{2}\Sigma[(y_1^{(\alpha)} - d_1^{(\alpha)}]^2 + (y_2^{(\alpha)} - d_2^{(\alpha)})^2 \quad (5)$$

Where y is current output and d is desired output of the fuzzy function.

Output of hidden layer in neural network

$$H_{yN}(k) = W_{iNJ}(k) + c(y_j) \quad (6)$$

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

Output of hidden layer in Jordan network

$$H_{yJ}(k) = W_{ij}(k) + c(y_j) \quad (7)$$

Fuzzy logic input

$$F^l = \bigcap_{i=1}^{n} F_i^l \quad (8)$$

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

Apply the complexity regularization method to optimize the number of hidden nodes from the observed data.

$$n= C\,(N/\,(d \log N))^{1/2} \quad (9)$$

Where n is number of hidden nodes, d is input dimension of the target function, N is the number of training pairs or observed pairs and C is constant. It is used to reduce the error value in the statistical analysis.

DIHFJANN output

$$F^l(H_{yN}(k)+H_{yJ}(k)) = O(y)_{FJN} \quad (10)$$

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

DIHFJANN mechanism with modified steepest gradient 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 network with the associated random weight initialization using (1) and (3)
5. Update the neural input vector x(k)
6. Update weight value
7. Compute the output of hidden in neural network H_{yN} (k) using (6)
8. Compute error minimum rate using (5)
9. If minimum error criteria are not reached then go to step 10 else goto step 5
10. Change the network structure randomly with more layers and nodes in layer
11. Apply the algorithm 1
8. Go to step 5 and continue until the end of the training data points
9. Compute the learning rates of each layer and update the weight matrices
10. Compute the output of hidden in Jordan network $H_{yJ}(K)$ using (7)
9. Save the values for particular weight initialization step for the iterative training and continue until the maximum weight-initialization number is reached.
10. Obtain the resultant weight initialization as the most excellent value for the training based on the chosen number of hidden layer fuzzy neurons.
11. Optimize the number of hidden nodes using complexity regularization through (9)
12. Dynamic improved hybrid fuzzy Jordan network and neural network output is obtained using (10)

The first order and second order statistics are utilized to handle the dynamic behavior of the intruder that is time varying features. Such kind of features is extracted from the packet data along with sliced time window. The first order statistics are such as mean, variance, Skewness and Kurtosis, second order statistics features are such as time varying moment, correlation and entropy features are computed. It is used to increase the classification accuracy in terms of higher intrusion detection rates in the dynamic network.

IV. Experimental Result

In this section the performance metrics of the proposed work is compared among existing 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 increase 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 used is 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 the performances are compared among networks for intrusion detection. Such kinds of methods are existing Hybrid Fuzzy Jordan Artificial Neural Network (HJANN) and proposed Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network (DIHFJANN). To increase the accuracy as well as efficiency, the dynamic parameters are utilized in this proposed system. From the experimental result evolved, it can be concluded that proposed methodology improved the prediction accuracy and also speeds up the convergence rate significantly. Hence proposed Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network (DHFJANN) 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,

Accuracy =

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

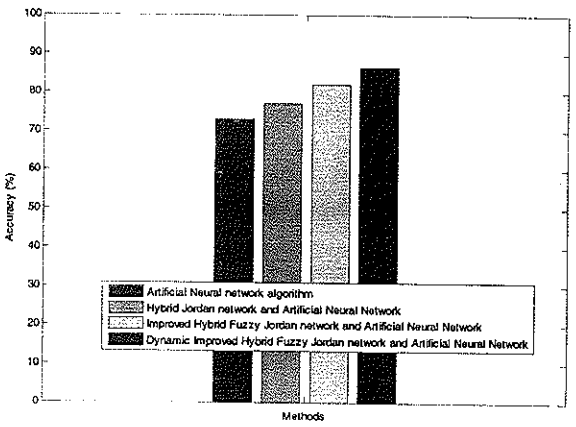

Figure : 1 Accuracy Comparison

From the Figure 2, it is clear that the proposed methodology provides better result than the existing approach by increased accuracy value. In this graph, the methods are such as ANN, HJANN, IHFJANN and DIHFJANN are plotted in the x axis and the accuracy values are plotted in the y axis. The accuracy value is low for the existing method of ANN, HJANN and IHFJANN. The accuracy value is increased significantly by using the proposed DIHFJANN. Thus, the proposed method is used to predict the intrusions efficiently. From the experimental result, it is concluded that proposed method is superior to existing system.

Precision

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

Precision =

$$\frac{\text{True positive}}{\text{True positive} + \text{False positive}} \qquad (7)$$

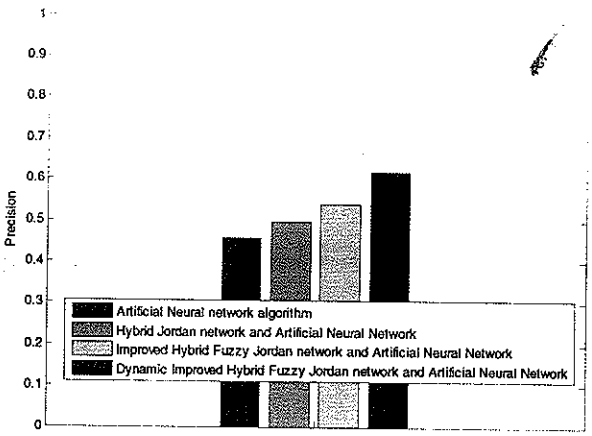

Figure 2 : Precision Comparison

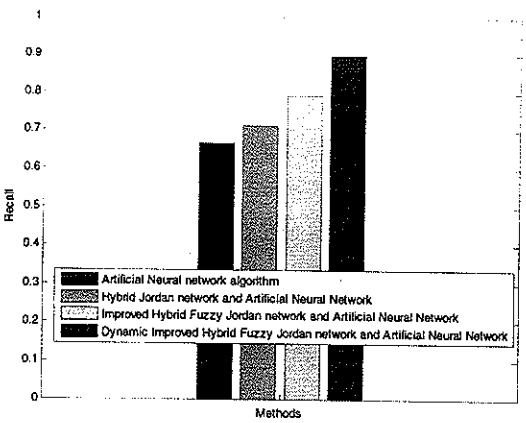

Figure 3 : Recall Comparison

From the Figure 3, it is observed that the proposed methodology provides better result than the existing approach as it has increased the precision value. In this graph, the methods are such as ANN, HJANN, IHFJANN and DIHFJANN plotted in the x axis and the precision values are plotted in the y axis. The precision value is low for the existing method of ANN, HJANN and IHFJANN. The precision value is increased significantly in the proposed DIHFJANN. Thus, the proposed method is used to predict the intrusions efficiently. From the experimental result, it is concluded that proposed method is superior to existing system.

Recall

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

$$\text{Recall} = \frac{\text{True positive}}{\text{True positive} + \text{False negative}} \quad (8)$$

From the Figure 4, it is observed that the proposed methodology provides better result than the existing approach as it has increased the Recall value. In this graph, the methods are such as ANN, HJANN, IHFJANN and DIHFJANN plotted in the x axis and the precision values are plotted in the y axis. The recall value is low for the existing method of ANN, HJANN and IHFJANN. The recall value is increased significantly in the proposed DIHFJANN. From the experimental result, it is concluded 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 :

$$\text{F-Measure} = 2.\frac{\text{Precision} . \text{Recall}}{\text{Precision} + \text{Recall}} \quad (9)$$

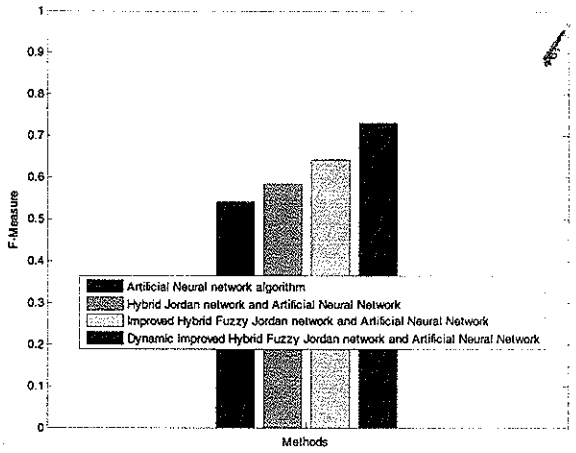

Figure 4 : F-Measure Comparison

From the Figure 4, it is 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, HJANN, IHFJANN and DIHFJANN plotted in the x axis and the F-measure values are plotted in the y axis. The F-measure value is low for the existing method of ANN, HJANN and IHFJANN. The F-measure value is increased significantly by using the proposed DIHFJANN. Thus, the proposed method is used to predict the intrusions efficiently. From the experimental result, it is inferred that proposed method is superior to the existing system.

Convergence iterations

From the figure 7, it can be proved that the proposed methodology provides better result than the existing approach as it speeds up the convergence rate. In this graph, the methods are such as ANN, HJANN, IHFJANN and DHFJANN plotted in the x axis and convergence rate values are plotted in the y axis. The convergence speed is reduced by using the existing method of HFJANN. The convergence speed is increased significantly by using the proposed DHFJANN. 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.

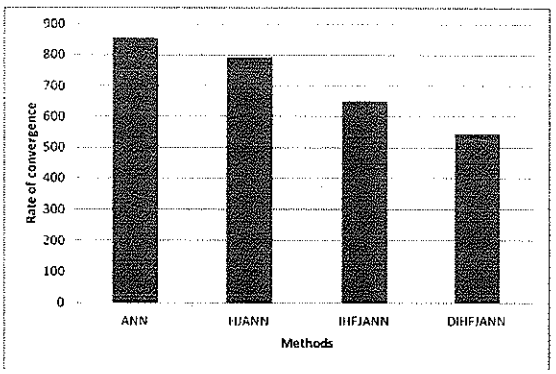

Figure 5 : Rate of Convergence

Table 1 : Comparison values for the Intrusion Detection System

Parameters	Methods			
	ANN	HJANN	IHFJANN	DIHFJANN
Accuracy	73	79	84	89
Precision	0.47	0.51	0.55	0.62
Recall	0.68	0.72	0.8	0.91
F-measure	0.55	0.62	0.65	0.74

The table 1 shows the different rate of convergence values for existing and proposed methods. The methods are ANN, HJANN, IHFJANN and DHFJANN approaches. The Dynamic Hybrid Fuzzy Jordan Artificial Neural Network based intrusion detection system's accuracy, precision, recall also f-measure rate is higher than the ANN, HJANN and IHFJANN approaches. From this experimentation, it is concluded that the Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network 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	857
2	HJANN	792
3	IHFJANN	650
4	DIHFJANN	545

The table 2 shows the different rate of convergence values for existing and proposed methods. The methods are ANN, HJANN IHFJANN and DHFJANN approaches. The Dynamic Hybrid Fuzzy Jordan Artificial Neural Network based intrusion detection system has the high speed of convergence rate compared to the ANN, HJANN and IHFJANN methods. From this experimentation, it is concluded that the Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network based intrusion detection system is effective and efficient rather than preceding method.

V. Conclusion

The proposed Dynamic Improved Hybrid Fuzzy Jordan Artificial Neural Network based method has improved the accuracy of prediction result in the intrusion detection system. This dynamic network is used to observe and discover the intrusions prominently by using the effective approaches. The convergence speed is increased significantly and the performance of the system is improved higher in the proposed technique. In future work, the optimization algorithm can be developed for weight optimization of both Jordan network and neural network. It can reduce the error rate significantly and improve stability of dynamic hybrid fuzzy Jordan neural network.

References :

[1] Ibrahim, Laheeb Mohammad, Anomaly network intrusion detection system based on distributed time-delay neural network (DTDNN), Journal of Engineering Science and Technology 5.4 (2010): 457-471.

[2] Dastanpour, Amin, and Raja Azlina Raja Mahmood, Feature selection based on genetic algorithm and Support Vector machine for intrusion detection system, The Second International Conference on Informatics Engineering & Information Science (ICIEIS2013), The Society of Digital Information and Wireless Communication, 2013.

[3] Ektefa, Mohammadreza, et al, Intrusion detection using data mining techniques, Information Retrieval & Knowledge Management,(CAMP), 2010 International Conference on. IEEE, 2010.

[4] Mabu, Shingo, et al, An intrusion-detection model based on fuzzy class-association-rule mining using genetic network programming, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on41.1 (2011): 130-139.

[5] Benamara, Lamia, and Clémence Magnien, Estimating properties in dynamic systems: the case of churn in p2p networks, INFOCOM IEEE Conference on Computer Communications Workshops, 2010. IEEE, 2010.

[6] Song, Qing, on the weight convergence of Elman networks, Neural Networks, IEEE Transactions on 21.3 (2010): 463-480.

[7] Staudemeyer, Ralf C, Applying long short-term memory recurrent neural networks to intrusion detection, Research Article SACJ No. 56, July 2015

[8] Hammer, Barbara, and Peter Tino, Recurrent neural networks with small weights implement definite memory machines, Neural Computation 15.8 (2003): 1897-1929.

[9] Koch, Robert, Mario Golling, and Gabi Dreo Rodosek, Behavior-based intrusion detection in encrypted environments, Communications Magazine, IEEE 52.7 (2014): 124-131.

[10] Youssef, Ahmed, and Ahmed Emam, Network intrusion detection using data mining and network behaviour analysis, International Journal of Computer Science & Information Technology 3.6 (2011): 87-98.

[11] Rehman, M. Z., and N. M. Nawi, Improving the accuracy of gradient descent back propagation algorithm (GDAM) on classification problems, International Journal of New Computer Architectures and their Applications (IJNCAA) 1.4 (2011): 838-847.

[12] Hofstede, Rick, et al, Towards real-time intrusion detection for NetFlow and IPFIX, Network and Service Management (CNSM), 2013 9th International Conference on. IEEE, 2013.

[13] Wu, Wei, et al, Convergence of gradient method with momentum for back-propagation neural networks, Journal of computational mathematics-international edition- 26.4 (2008): 613.

[14] Chein-Shan Liu, "Modifications of Steepest Descent Method and Conjugate Gradient Method against Noise for Ill-posed Linear Systems", Volume 2012, Year 2012 Article ID cna-00115, 24 pages 10.5899/2012/cna-00115 Research Article.

[15] Chaudhary, Alka, Neuro-fuzzy based intrusion detection systems for network security." journal of global research in computer science 5.1 (2014): 1-2.

AUTHOR'S BIOGRAPHY

Dhivya Arun received M.E. degree in Embedded Systems from Karpagam University in the year 2011, respectively. She has also worked as Assistant Professor of Information Technology at Karpagam Institutions from 2005 to 2014. Her research interests are in Artificial Neural Networks. She is winner of "Professional Knack" at Infosys in the year 2012.

Dr. S.N. Sivanandam has a bachelor's degree in Electrical Engineering, a master's degree in Power Systems and Ph.D. in Control Systems. He has over 41 years of teaching and research experience in the fields of Control Systems, Digital Systems, Neural Networks, Fuzzy Logic, Genetic Algorithm, Data Mining, Modeling and Simulation, Multidimensional Systems and Knowledge based Systems. He received Best Teacher Award in the year 2001 and Dhakshina Murthy Award for Teaching Excellence from PSG College of Technology and the CITATION for best teaching and technical contribution in the Year 2002 from Government College of Technology,Coimbatore.