Multiuser Authentication and Intruder Detection using Neural Computing

Suma Santosh
Assistant Professor
Dept of TCE
KSIT Bangalore

Savita S.Biradar
Assistant Professor
Dept of TCE
KSIT Bangalore

ABSTRACT
The objective of the paper is to mainly detect the Intruder activity in security systems and to authorize the correct person to make use of resources which is done using Artificial Neural Networks. Security is a broad topic and covers many issues. Malicious people trying to gain some benefit, attention, or to harm someone intentionally cause most security problems. An Intrusion Detection System detects attacks as soon as possible and takes appropriate action. ANN provides Multilevel, Multivariable security system, which can fulfill the strong requirement of security. Apart from providing security, ANN will have the capability to detect, if any intrusion happens.

General Terms
Artificial Neural Networks

Keywords
ANN, multilayer feed forward network, Error back propagation algorithm, Intrusion detection..

1. INTRODUCTION
An Artificial Neural Network (ANN) also called Neural Network is an information-processing system that is inspired by the way biological nervous systems, such as the brain process information. The key element of this paradigm is the novel structure of the information processing system. It is composed of a large number of highly interconnected processing elements (neurons) working in parallel to solve specific problems. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition, signal processing and data classification etc., through a learning process. Hence neural networks take a different approach to problem solving than that of conventional computers, which use an algorithmic approach. They follow a set of instructions (program) in order to solve a problem. Conventional computers cannot solve the problem unless the specific steps they need to follow are known. Whereas neural networks cannot be programmed to perform a specific task. They process information in a similar way the human brain does. Learning in biological systems involves adjustments to the synaptic connections that exist between the neurons. This is true of neural networks as well. ANNs have been applied to an increasing number of real-world problems of considerable complexity. Most important advantage of ANN is in solving problems that are too complex for conventional technologies. In general, because of their abstraction from the biological brain, ANNs are well suited to problems that people are good at solving, but for which computers are not. [1] The network is designed first. With the help of the learning process and the weights, the fault prone connection can be detected. ANN is needed because of the current technology limitations, like Speed, Intelligent & Fault tolerance. The computational speed of ANN is very fast compared to other technologies due to its parallel-distributed nature of processing. It has the power of intelligence because of adaptability. Since ANN is composed of large number of simple computational units, operating in parallel and the training algorithm can organize these existing computational units in such a way that the network acquires the potential to provide fault tolerance. [2]

2. OVERVIEW OF ANN
Neural network simulations appear to be a recent development. However, this field was established before the advent of computers, and has survived at least one major setback and several eras. Many important advances have been boosted by the use of inexpensive computer emulations. Much is still unknown about how the brain trains itself to process information. The neural networks are deduced based on the essential features of neurons and their interconnections. Then a computer is programmed to simulate these features.

2.1 Model of an Artificial Neuron
The fig 1 shows the model of an artificial neuron. The three basic elements of this model are,

2.1.1 A set of synapses or connection links
These are characterized by a weight (or strength) of its own. Specifically a signal "Xi" at the input of a synapse "i" connected to a neuron "j"is multiplied by the synaptic weight "Wij".

2.1.2 An adder
For summing the input signals weighted by the respective synapses of the neuron, to produce the summation (net)i.

2.1.3 An activation function
For limiting the amplitude of the output of a neuron. This function also referred to as a "squashing" function in that it limits (squashes) the amplitude range of the output signal (Oi) to some finite value.

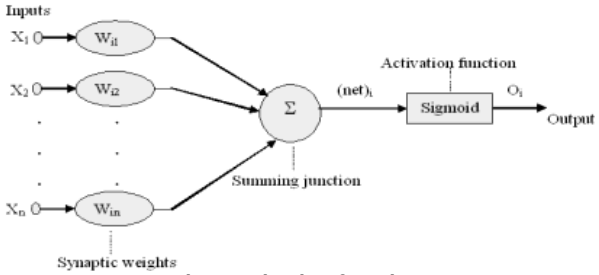

Fig 1 Activation function

The behavior of ANN depends on both the connection weights and the input-output function (activation function) that is specified for the computational elements (active nodes). The most popular form of activation function used in ANN construction is the *'Sigmoid'* function. It is defined as a strictly increasing function that has soft threshold and that which exhibits a graceful balance between the linear and non-linear characteristics. The graph and the function is given by,
$Oi = 1/ (1+\exp (-\lambda . neti))$

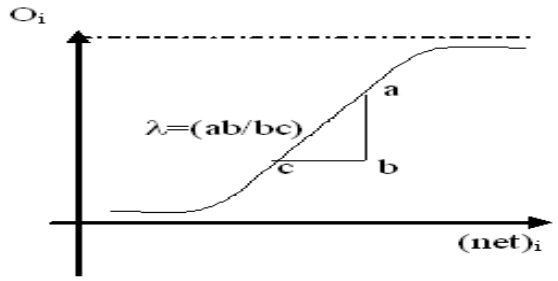

Fig. 2 Sigmoid function

3. PROPOSED METHOD

This is a technology based on the principle of replication of brain in terms of architecture and processing operation. Architecture is a physical existing module, while processing is a methodology sometimes called learning rule or to get the result. In the ANN processing there are two different phases, one is called Learning Phase and another Test Phase similar to human brain.

3.1 Multi-Variable Parameters and their Hierarchy in Security System

The multivariable parameters introduced in the paper are

- Time of intrusion (Year, Month, Date, Hour, Minutes, Seconds)
- Identification inserted by intruder (Length check)
- Time taken in inserting the Identification
- No of trails taken by intruder before un authentication declared as shown in Fig 3.

3.2 Protection of Reset Process

The Reset Process allows the valid user to change the password, if any intruder activity takes place and also to change the password of all three identities according to users wish. If the intruder fails to access the Resource, and attempts to enter the reset process to change the identities, First the intruder should enter the Reset identity followed by P.I.P and S.I.P of the Resource, which makes the intruder difficult to handle the Resource. So it can be said, resetting the identity itself is protected by all other identities. If once un-authentication is detected it is not possible to utilize the resource even by right person. So remedy is to reset the system as shown in Fig. 4.

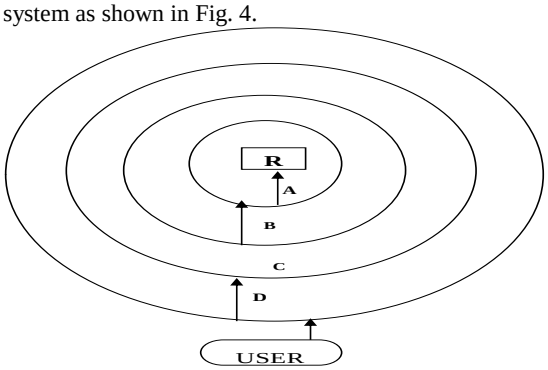

Fig. 3 Multivariable Parameters

A- Authentication Protection
B- Trail Protection
C - Inserting Time Protection
D- Length Protection
R- Resource being protected

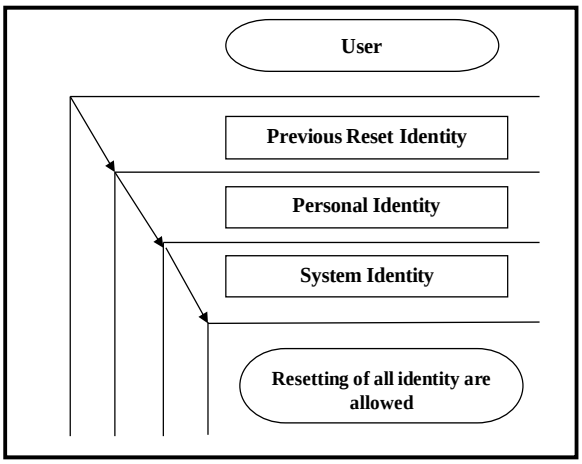

Fig. 4 Reset Process

3.3 Proposed feed forward ANN architecture

ANN is also referred as "parallel distributed processing system". Here Gaussian distribution is used because it offers high fault tolerance capability as compared with that of uniform distribution since the random values are much apart from each other. Initially all the connection strengths are multiplied with the corresponding inputs and the result of this becomes the input to the hidden layer processing nodes. The active hidden layer performs accumulation and mapping operation on these inputs. The mapping of the accumulated result is required so that it could remain a bound number. [4] Output of hidden layer nodes are multiplied with the random weights selected for the outer layer. This becomes the input to the output node, which is also active. Accumulation and mapping is done at this node. Fig 5 shows ANN architecture design. The error function is defined to check the co-relation. If the error is not satisfying according to required criteria (less than or equal to threshold), the learning rule will take charge of weight adjustment in right direction as to reduce the error. Now these adjusted weights become the connection strengths for the next generation processing. The further operation is repeated as in the first generation till error satisfies required criteria.

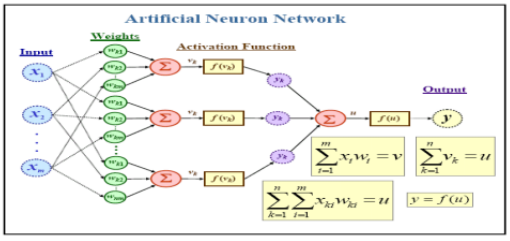

Fig. 5 Artificial Neuron Network Architecture Design

3.4 Training/ Learning of ANN

The idea behind learning in Neural Network is that, the output depends only on the activation, which in turn depends on the values of the inputs and their respective weights. The initial weights are not trained with respect to the inputs, which can result in error. Now, the goal of the training process is to obtain a desired output when certain inputs are given. Since the error is the difference between the actual and the desired output, the error depends on the weights, and weights have to be adjusted so as to minimize the error. The error function is defined for the output of each neuron [5] as,

Error = desired output – actual output.

The Delta Rule: This is one of the most commonly used rule. This rule is based on the simple idea of continuously modifying the strengths of the input connections to reduce the difference (the delta) between the desired output value and the actual output of a processing element. This rule changes the synaptic weights in the way that minimizes the mean squared error of the network. This rule is also referred as Least Mean Square (LMS) Learning Rule. [10]

The back-propagation algorithm (Rumelhart and McClelland, 1986) is used in layered feed-forward ANNs. [4]. this means that the artificial neurons are organized in layers, and send their signals "forward", and then the errors are propagated backwards. The network receives inputs by neurons in the input layer, and the output of the network is given by the neurons on an output layer. There may be one or more intermediate hidden layers. The back-propagation algorithm uses supervised learning. In this case the algorithm has to be provided with examples of the inputs and outputs that the network has to compute, and the error (difference between actual and desired results) is calculated. [7]

New weight = Previous Weight + Changed Weight

$$w'_{ij} = w_{ij} + \Delta w_{ij}$$

4. COMPARISON

Table1: Comparison of supervised learning and unsupervised learning

Supervised learning	Unsupervised learning
Teacher will be present	There will be no teacher
Network is supported with both input and desired output	Network is supplied with only input
Unable to provide Real-time response	Able to provide real time response
Global information is required	Local information is required
Learning vector quantization is used	Learning matrix is used

5. EXPERIMENTAL RESULTS

This section gives all the experimental results that are observed during the execution of the paper. Fig 5 describes about Learning phase identities when person enters into matlab workspace and enter secu_pr.Then the system will ask to enter all the 3 identities. Once the identities are correct the resource will be available which is shown in Fig 6.

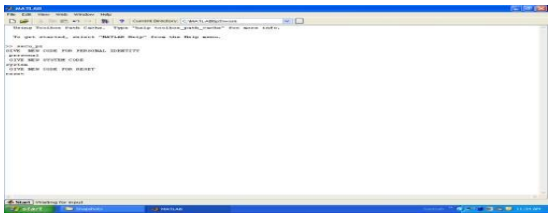

Fig 5: Learning Phase Identities

Fig 6: Authorized person

The error gradually decreases with the number of iterations. Fig 7. Shows how the neural network error decreases as the iterations proceed for the three identities.

Fig 8 shows the neuron architecture for the three identities. Fig 9 and Fig 10 show the graph of variation in the initial weights and trained weights at Hidden and Output layer respectively describing that the machine has learnt.

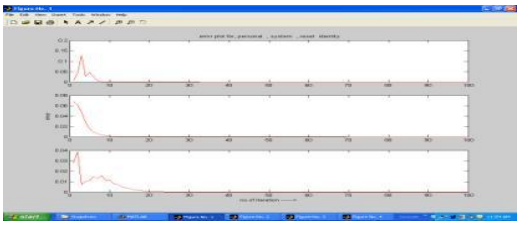

Fig. 7.Error and Number of Iterations of Test Phase identities

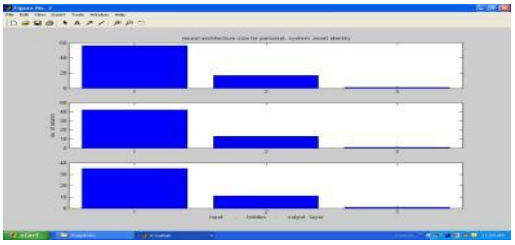

Fig.8.Neuron Architecture of Identities

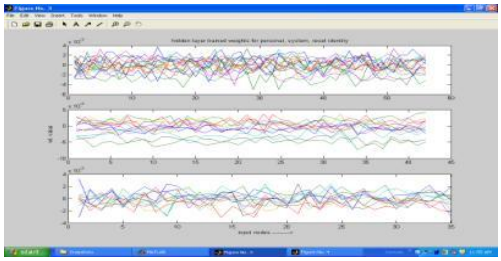

Fig 9 Hidden Layer Trained Weights

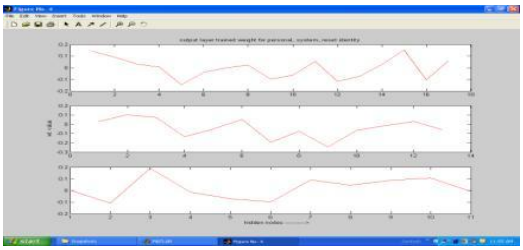

Fig 10. Output Layer Trained weights

6. CONCLUSION

Artificial neural networks are inspired by the learning process that takes place in biological systems. Neural networks represent a new computing environment based on the parallel architecture of the brain. They can be trained to produce an accurate output for a given input. The Network posses the advantages of simple computations, fault tolerance, parallel processing, robust with respect to node failure. In this paper, the concept of Error Back-Propagation Learning algorithm has made a break through in supervised learning of layered neural network. This paper proves the Protection of Resource by intruder.

In this paper, security and intrusion detection is developed by using multilevel, multivariable parameters. The advantage of building the architecture to the user desire level, and hiding learning phase from the intruder. The only limitation focused in this paper is, training is slow, may converge to a local value not to global.

Finally, it can be conclude that the paper "Multiuser Authentication and Intruder Detection Using Neural Computing" has been proven successfully the ability of the network to protect information and system resources with respect to confidentiality and integrity.

7. REFERENCES

[1] Survey on Intrusion Detection Methods,Sanoop Mallissery, Jeevan Prabhu, Raghavendra Ganiga 3, Proc.of 1nt. Con/, on Advances in Recent Technologies in Communication and Computing 2011

[2] A Neural Network Based Anomaly Intrusion Detection System, Sufyan T. Faraj Al-Janabi and Hadeel Amjed Saeed, 2011 Developments in E-systems engineering.

[3] Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks Mohammad Reza Norouzian, Sobhan Merati ISBN 978-89-5519-155-4.

[4] Jacek M.Zurada, Introduction to Artificial Neural Systems, Sixth Jaico Impression, 2003.

[5] Artificial Neural Network Learning: A comparative Review, by Costas Neocleous, Christos schizas, Lecture Notes in Computer Science; Vol. 2308, 2002, Pages: 300 - 313.

[6] Aurobindo Sundaram, An Introduction to Intrusion Detection, 3rd edition 2000.

[7] Supervised Learning in Feed forward Artificial Neural Networks by Robert J.Marks, MIT Press, 1998.

[8] Lin. M. Miikkulainen, Intrusion Detection with Neural Networks 2nd edition 1995.

[9] S.Haykin, Neural Networks: A comprehensive Foundation, Macmillan College Press, New York, 1994.

[10] J. Hertz, A. Krogh, and R.G. Palmer, Introduction to the theory of Neural Computation, Addison-Wesley, 1991.