An Innovative Instruct Dynamic Intrusion Detection System with Particle Swarm Optimization and Radial Basis Functions

Dr. M.V. Siva Prasad
Professor, CSE department, Anurag Engineering College, Kodad

Abstract— This research paper is an elaboration of Incremental Radial Based Function Neural Network model with Particles Swarm Optimization (IRBF-PSO) in Intrusion Detection System. This system is helpful to find the most featured misuse and anomaly detection. RBF network is most popular real-time classifier method. RBF method comprises of mostly analysis and the thorny part is finding the right weights and bias values for dynamic systems. The intrusion detection system has become highly dynamic. Many large or small enterprise systems are still facing with different problems in this area with dynamic form. So the main objective of my work is to employ Particles Swarm Optimization to detect the right weight and bias values for RBF method.

In this method, apart from training with existing data and information for design, there is a need to extend or redesign the existing system to identify different pattern types and modulate the system using PSO with new patterns. After experimentation, this method has improved to identify the difficulty in anomaly detections and reduce the rate of false alarm and fail cases.

Key Words—Incremental method, intrusion detection system, particles swarm optimization and radial based.

I. INTRODUCTION

Amid growing connectivity between computers, the protection of computer networks plays an intentional role in now a day's computer systems. Major in that, detecting intrusions in network has become one of the most significant parts to obstruct the abuse of network resource by aggressors.

The securities are generally divided into various levels.

Intrusion Detection System (IDS) is the vital part in securities. The major job of the IDS‟ is to not only detect the intrusions, but also to monitor the security issues and the network traffic. In broad, the conventional intrusion detection relies on the wide facts of security experts, in meticulous, on their acquaintance with the computer system to be protected. Normally it's placed after firewall security and filters. Fig. 1 depicts the high level representation. We can design the Intrusion Detection Systems in two ways: One way is Misuse Detection method, which uses patterns to detect the presence of known attacks. Another way is Anomaly detection approach which builds a model of normal behavior of the system. In this paper we discuss about Misuse Detection method [1]-[5].

Many researchers have designed different IDS systems to compute major challenges using different classifiers methods. Any system behavior that does not match with this model is reported as Anomaly.

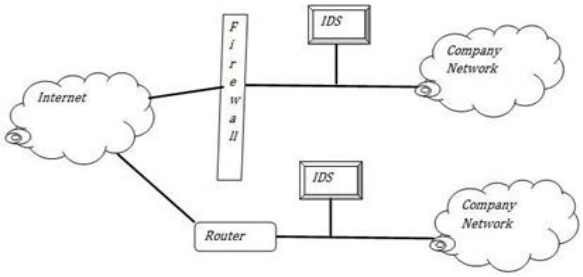

Fig.1.IDS Representation

While anomaly detection typically utilizes threshold monitoring to indicate when a certain established metric has been reached, misuse detection techniques frequently utilize a rule-based approach using computing methods. The use of comprehensive rules is critical in the application of expert systems for intrusion detection.

Most current approaches to the process of detecting intrusions utilize some form of rule-based analysis. Rules system examination based on sets of existing rules that are provided bya system organizer are automatically created by the system, or both. The use

of expert system techniques in intrusion detection mechanisms was a significant milestone in the development of effective and practical detection-based information security systems. Expert rules are generated based on different methodologies like Data Mining, Neural Networks methods, Soft Computing et al. Most of the traditional methods for generating a rule-set is based on decision tree (ID3 algorithm). It‟s been used by many researchers from earlier days to the present days. AfterID3,a number of advanced decision tree algorithms were proposed by various research teams. But, the most successful rule based algorithm is C4.5 (SEE 5.0). The next most popular rules-set-generation methods are Neural Networks techniques. The neural network consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. The result of the transformation is determined by the characteristics of the elements and the weights associated with the inter connections among them [1]-[5].

In the Neural Network, one of most popular and traditional algorithm is Back propagation (BP) Algorithm. Idea behind BP algorithm is quite simple, the output of NN is evaluated against desired output. If the results are not satisfactory, connection (weights) between layers are modified and process is repeated again and again until error is small enough. Simple BP example is demonstrated in this paper with Neural Network architecture is also mentioned. New implementation of Back Propagation [BP] algorithm is emerging and there are few parameters that could be changed to improve performance of BP Back. In the Neural Network, one of the most popular and traditional algorithm is Back propagation (BP) Algorithm. Idea behind BP algorithm is quite simple; the output of NN is evaluated against desired output. If the results are not satisfactory, connection (weights) between layers are modified and process is repeated again and again until error is small enough. Simple BP example is demonstrated in this paper with Neural Netwok architecture is also mentioned. New implementation of BP algorithm is emerging and there are few parameters that could be changed to improve performance of BP Back.

Radial Basis Function (RBF) Networks consists of a single hidden layer of locally-tuned units which is fully interconnected to an output layer of linear units. Sum of radial basis functions are typically used to approximate given functions. This approximation process can also be interpreted as a simple kind of neural network. RBFs are also used as a kernel in support vector classification. RBF networks have strong tolerance to input noise, which enhances the stability of the designed systems. Therefore, it is reasonable to consider RBF network as a competitive method of nonlinear controller design. However, the drawback of RBF is that it treats all the input parameters with equal importance. RBF networks act as local approximation networks and the network outputs are determined by specified hidden units in certain local receptive fields, while BP networks work globally and the network outputs are decides by all the neurons. It is characterized by single best approximation, only local minimum, less calculation and fast learning, and is widely applied to pattern classification, system identification and functional approximation. Our research proposes using Particle Swarm Optimization-RBF NN in image retrieval process using local minimum (pBest) and global minimum (gBest) [6]-[15]

Particle Swarm Optimization (PSO) is a recently developed numerical method for optimization, which is simple, easy to apply and has a strong smart background, and it has been used in many fields such as function optimization, and pattern recognition. PSO algorithm [15] is used in the training of RBF neural network. The Proposed PSO-RBF neural network method is uses PSO algorithm to proceed global dynamic searching, and used in RBF neural network to proceed the local optimizing. After closer observation and research in point of the local and global minimum finding using PSO algorithm, PSO uses only one Swarm. Swarm is a collection of particles. The weight and bias values for RBF method are detected correctly by Particles Swarm Optimization. Here, this existing trained data/information is used to design the right system. Need to broaden or redesign system when identifying different patterns types and modulate system using PSO with new patterns. In the proposed system, we use a new method called incremental instruct dynamic intrusion detection system using PSO-RBF (IRBF-PSO).

II. BACKGROUND

Many researchers have various approaches in using neural networks for intrusion detection. A couple of

groups created keyword count are based on misuse detection systems with neural. The data that they presented to the neural network consists of attack-specific keyword counts in network traffic in old days. Such a system is close in spirit to a host-based detection system because it looks at the user actions in a different approach, researchers created a neural network to analyze program behavior profiles instead of user behavior profiles. This method identifies the normal system behavior of certain programs, and compares it to the current system behavior. This led to the development of a network-based neural network detection system in which packet-level network data was retrieved from the database and then classified accordingly into nine packet characteristics and presented to a neural network. This method is different from our proposed system as Cannady proposed a system of detection on packet level, where as we use a time-window method. Our method allows us to generalize input further than the Cannady‟s method enabling us to recognize longer multi-packet attacks. In addition, we ar modeling the network traffic in our preprocessing steps, we only need to look at three packet characteristics to identify aggregate trends. Self-Organizing Maps (SOMs) have also been used as anomaly ntrusion detectors. In that work, SOMs are used to cluster and then graphically display the network data for the user to determine which clusters are contained with attacks. Using SOM as a clustering method for MLP neural networks is an efficient way of creating uniform, grouped input for detection when a dynamic number of inputs are present[10]. But still some issues in Neural Network system with hidden layer complexity are pending. Using Radial Based Function Neural Network, solve this existing hidden layer complexity as RBF uses only one hidden layer.

Even though there are researchers analyzing the development of RBF Network training, but research on training of RBF Network are lacking in development of point parameter adjustment.

A recent algorithm - Particle Swarm Optimization (PSO), which is adapted from decentralized and self-organized systems in nature, such as choreography of a flock of birds and school of fish. It is a population-based algorithm, in which individual particles work together to solve a given problem. In PSO, physical position is not an important factor. The population (or swarm) and the member particles are initialized by assigning random positions, velocities, and potential solutions are then „flown‟ through the hyperspace [7]-[10].

Using RBF-PSO method is not able to solve the new attackers in current and future. In our research new methodology is helpful to find the new pattern of attackers.

III. PROPOSED METHODOLOGY

This paper proposes a methodology to improve the accuracy of the classification process, to reduce the amount of data needed for processing and to improve the false alarm rate by using the Radial Base Function Neural Network (RBF-NN), Radial Base Function Neural Network with PSO. (PSORBF) and Incremental Radial Base Function Neural Network with PSO (IRBF-PSO). Especially our research proposed a dynamic approach for finding false alarm rate using Incremental Radial Base Function with PSO. Our proposed method shows more accuracy compared with existing methods.

This methods explains the methodology followed during the research on classification based on the decision tree classifier and its various aspects related to the training size and pruning. Fig. 2 explains the conceptual flowchart of the full methodology. The training dataset for the decision tree is different as it is non-parametric classifier. Decision tree was generated using See5 decision tree software. The main advantage of See5 is that it can convert a decision tree into classification rules[2],[3].The decision tree generated from the DARPA data was then converted to classification rules to form a knowledge base. The knowledge base created from this process was then used in further classification of the IDS attackers‟ signature. Basically four types of classification were performed and one type novel process computing classifier:

- Radial Base Function Neural Network.
- Radial Base Function Neural Network with PSO.
- Incremental Radial Base Function Neural Network with PSO.

Finally the accuracy assessment was done for all the classification methods using different standard metrics considering mainly the following parameters:

- Classification rate of attackers
- User accuracy
- Procedure accuracy
- Overall accuracy

Evaluation of the performance accuracy is assessment of the proposed method. Finally the proposed classifiers to reduce the amount of data needed for processing and false alarm rate in future for any type of new attacker patterns.

Final testing on Defense Advanced Research Projects Agency (DARPA) data set 1998, 1999 and 2000, conclude best automation process of the IRBF-PSO for IDS.

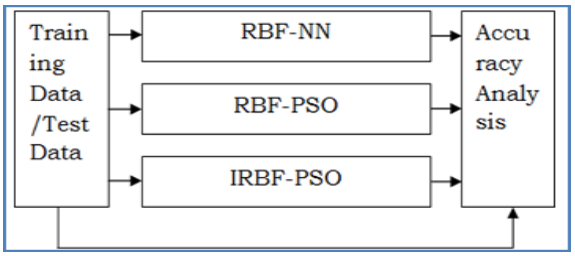

Fig.2.Proposed methodology

The data set has 41 attributes and one class label. The actual full data set contains 743MB uncompressed millions of records. Actual data set contains 22 attack types. Those attacks can be prominently divided into four groups [3]: Denial of Service (DoS), Unauthorized Access from Remote Machine (R2L), Unauthorized Access to Local Super User. (U2R) and Surveillance and Other Probing (Probing).

IV. RADIAL BASE FUNCTION NEURAL NETWORK

Radial Basis Function (RBF) is one of the methodology used in the Neural Network (NN)[16],[17]. It is similar to feed-forward neural network which consists of three layers. Following are layers that are involved in the RBF Neural Network:

- Input Layer
- Hidden Layer
- Output Layer

A Few other significant points in RBF NN are:

- Centroid values for hidden Nodes,
- Process way in hidden node,
- Weights and Bias values.

Generally, in input layer there is no processing. The hidden layer uses Centroids and the Gaussian function for finding output value. Between Hidden layer and output layer a linear function is used to find the output. Input Layer is number of input vector size of the nodes, Input vector is:

$$xd = (x1, x2, x3, \ldots\ldots, xd) \quad (1)$$

In this paper, we are giving 41 attributes as input vector. Hidden layer is the significant layer in RBF NN, we use activation function in this layer. Centroids values are assigned to each hidden node. Normally, it is defined in two ways [18]:

Randomized: Assign randomly generates input dataset to Hidden nodes.

K-Means Clustering: this algorithm is best suitable to find the Centroids values.

In our research, K-Means is used to define the Centroids and assign these values to hidden node. It is defined as 21 types of output attacks. In this research, classification is done as four classes or output nodes. This research is designed41-42-4 RBF Neural Network. Fig. 3 is sample RBF Neural Network shown. It's shown with 3 layer architecture.

Different functions are available, below are major activation functions:

Gaussian Functions: $\emptyset(r) = exp(-r^2)$ (2)

Multi-Quadric Functions: $\emptyset(r) = (r^2+\sigma^2)^{1/2}$ (3)

Generalized Multi-Quadric Functions:

$\emptyset(r) = (r^2+\sigma^2)^{\beta}$ (4)

Inverse Multi-Quadric Functions:

$\emptyset(r) = (r^2+\sigma^2)^{-1/2}$ (5)

Generalized Inverse Multi-Quadric Functions:

$\emptyset(r) = (r^2+\sigma^2)^{-\alpha}$ (6)

ThinPlateSplineFunction: $\emptyset(r) = r^2 ln(r)$ (7)

Cubic Function: $\emptyset(r) = r^3$ (8)

Linear Function: $\emptyset(r) = r$ (9)

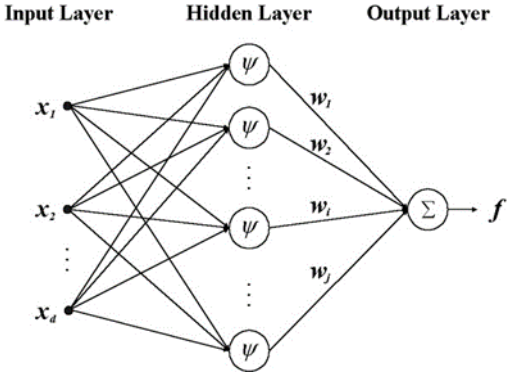

Fig.3.SampleRBFneuralnetwork

This research mainly focuses on Gaussian Functions in RBF NN in many applications, because of more advantageous and useful analytic properties when compared with other activation functions. Final output function is specified below (10). The sum (x) output:

), in this Gaussian Function,d is distance between centroid and input vector. σ is the standard deviation. Our research is tested with different positive and negative values starting from 3.$Wi$is weight values. Weight values are real values, which are defined using different methods. One method selects the weights randomly.

$$y(x) = \sum W e^{-d*d/2\sigma^2} + bias\_value \quad (10)$$

$e^{-d*d/2\sigma^2}$ i s a part of the (10),

V. RADIAL BASE FUNCTION NEURAL NETWORK WITH PSO

Particle Swarm Optimization (PSO) is a best technique to find numerical values in any optimization problem. PSO shares many similarities with evolutionary computation techniques such as Genetic Algorithms (GA). The system is initialized with a population of random solutions and searches for optimal by updating generations. Particles are initialized with random position, later it is moved to right direction to find optimization values. Particle Swarm Optimization is collection of particles and one Swarm. Swarm is collections of particles. Following are the properties of Swarm and Particle:

1) PSO use sonly one Swarm.
2) Characteristics of a Swarm

- Distributed, no central control or data source;
- Limited communication
- No(explicit) model of the environment;
- Perception of environment(sensing)
- Swarm is a collection of particles.
- Numberofparticlesusuallybetween10and50
- Each Swarm has Global Best Position and Global Best Error.

Each particle has five properties:

1) Position: Random values are between min and max values MIN and Max values are defined between-10 and 10.
2) Error: Using initial position values compute K-Means RBF network. Find the MSE values.
3) Velocity: Random values.
4) Best Position: Initial position values set is Particle Best Position
5) Best Error: Initial position error is Particle Best Error.

Fig.4.SampleRBFneuralnetwork.

```
Algorithm PSO ()
{
// Initialization with random values each particle
        Iteration: number of Iterations defined constant value.
        W: defined as weight value, C1 and C2 Local and Global cognitive, r1 and r2
random constant.
   Initialization Particle with Randomly Position and Velocity. Using position values
specified Error.
  Initial Position value is defined best position and error defined as best error.
  Defined Swarm with BestError and BestPosition based particle definition.
While (epoch<iterations)
  {
          Randomly select particle, copy particle to currP values.
            Find new velocity using below formal:
            newVelocity(j) = (w*currP.Velocity(j))+(c1*r1*(currP.bestPosition(j)-
        currP.Position(j)))+(c2*r2*(currP.bestGlobelPosition(j)-currP.Position(j));
        NewPosition=CurrentPosition+NewVelocity;
        Using new positionfind the MSE values.
            If NewPositionMSE<GError then
                    Swarm and Particle moved to new position;
            Else if NewPositionMSE<Error then
                    Particle is moved newPostion;
          Else
                    Not moved to new position;
            End if;
  };
};
```

Fig. Sample RBF neural network

Initial Swarm is defined with Best Global Position and Error based on all defined Particles. Particle movement is based on the given algorithm shown in Fig. 4. Particle is moved either completed epochs or reached. RBF-PSO is best to find the attackers based on comparison with basic RBF system. More analysis and results are discussed in next section which is performance analysis. Mostly, IDS systems is facing dynamic facing issues with new patterns. Hence it is always not possible to satisfy with existing PSO weight and bias for new patterns. Hence this research proposed new methodology for dynamical change of values of the system. Proposed methodology is explained in below section.

VI.INCREMENTAL RADIAL BASE FUNCTION NEURAL NETWORK WITH PSO

IRBF-PSO is a newly proposed method. It is based on dynamic behavior r of the datasets.

Fig.5shown proposes a methodology of process flow. Mainly this research focuses on one of the significant point in classification algorithms, which is not always possible to get complete accuracy with test data. In this method, the vital point is the distance parameter between new data set and existing trained dataset. If any new data set is less than the distance (d) threshold, then it is not required to redesign the weight values of the new data set. Here, will find the class for new data set using the manual process of the system. $n_i$means new dataset and $t_i$means training dataset are defined as threshold.

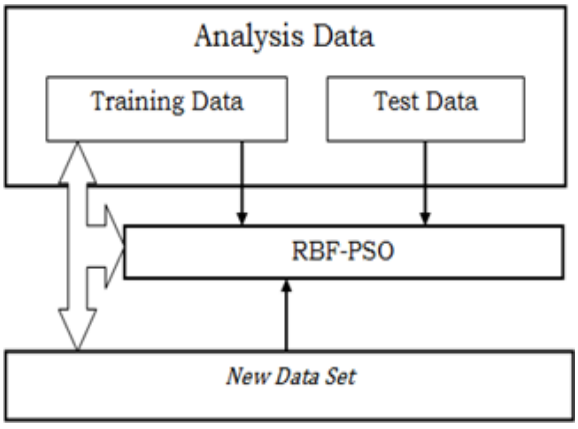

Fig.5.MethodologyofnewproposedIRBF-PSO.

Based on new algorithm Fig. 6, new data set processes in right way with our new proposed method. Compare results is done in below section

```
Algorithm IRBF-PSO()
{
New data set;
Find the distance d using (12);
If θ < d then
   Test using existing system;
Else
Call pso (); // figure 4.
};
```

Fig.6.AlgorithmforIRBF-PSO.

VII. ACCURACY ASSESSMENTS

In our research analysis, existing system in IDSs are not designed with better accuracy for dynamic environment. Mainly, research continued in this point and elaborated dynamic system designs for dynamic IDS systems. Final, our research demonstrated IRBF-PSO accrued accuracy for existing attackers and for new pattern attacker also.

Fig. 7 shows the accuracy of the existing and proposed classifiers methodologies using different training set sizes on the test data sets. Here main important point in below results is IRBF-PSO consistence maintain even test data set is increasing in any point. Based on this results our proposed method works for new data sets also in future.

Other methods inconsistence for different test data sets in different way. But PSO-RBF is accuracy more compared with basic RBF method. Here basic RBF method used 1000 iterations. Mainly Weight and Bias values finding using PSO is placed advantages compare with other existing methods. In our analysis is used the Strand Deviation with 3 for all datasets, when we have compared with other values means1, 2,4and 5 got better results for 3.

In PSO used Wasstrand1 and $r1$and $r2$ used value1. $C1$ and $C2$ used 0.812.

TABLEI: Test Accuracy for Different Datasets

#Training Data	#Test Data	RBF	PSO-RBF	IRBF-PSO
950	50	76	86	86
800	200	72.5	81.5	86.5
700	300	65.33	75.66	85.33
500	500	61.6	68.8	85.2
400	600	53.83	62.24	84.66
200	800	51.875	52.125	83.75

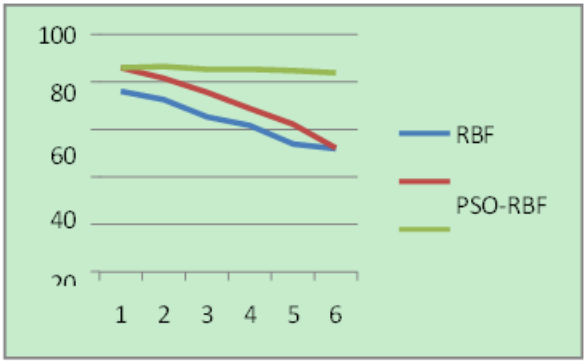

Fig.7.Graphical representation

VIII. CONCLUSION

Intrusion Detection System is more important in network and application systems. Here more difficult job is find type of attackers in IDS system. From the past decade, because of the growing network usage and security problems. The accuracy assessment of IDS system design using Radial Basis Function Neural Network, Radial Basis Function with Particle Swarm Optimization and Incremental Radial Basis Function with Particle Swarm Optimization are emphasized in the study [19]. Used all aspects of pattern of features are covered, total 41 features. Radial Basis Function Neural Network produced 76, 72.5, 65.33, 61.6, 53.83 and 51.875% of test accuracy for different sample of test data sets. Here Centroid values are defined using K-Means Clustered algorithm. This is due weight and bias values are defined using random values and used 1000 iterations. Based iterations on accuracy are changed. But still accuracy is not much different, need to improve by defining proper weights and bias values. Using Particle Swarm Optimization method, defined weight and bias values optimally. PSO is best approach to compute complex functions for optimized values. Using PSO, constructed Radial Basis Function which produced 86, 81.5, 75.66,68.8,62.24and52.125%test accuracy. The drawback of PSO is, it takes only single dimension this causes the machine not more dynamic, and when its new patterns of attacker the existing weight and bias values are not satisfied to find the attacker type. Existing weaknesses are resolved using Incremental Instruct Dynamic Intrusion Detection System using PSO-RBF methodology. This method achieved best accuracy results for different dynamic cases Incremental Radial Basis Function with PSO produced following accuracy for test data: 86, 86.5, 85.33, 85.2, 84.66 and 83.75%.

Hence, the above results demonstrate that Incremental Instruct Dynamic Intrusion Detection System using PSO-RBF computing classifier surpasses other classification methods. IRBF-PSO computing classifier method gives more accuracy in all other dynamic change applications.

REFERENCES

[1] U.M.Fayyad, GPiatetsky-Shapiro, P.Smyth, and R. Uthurusamy, Advances in Knowledge Discovery

[2] And Datamining, Menlo Park, CA: AAAI/MIT Press, 1996.

[3] E. M. Hassib, A. O. A. Elgwad, and A. I. Saleh, “A hybrid intrusion prevention system for web database security,” International Journal of Engineering Science and Technology, vol. 2, no. 7, pp. 2745-2762,2010.

[4] M.Crameretal.,“New methods of intrusion detection using control-loop measurement,” in Proc. the Technology in Information Security Conference (TISC), 1995, pp. 1-10.

[5] L. Fu, “A neural network model for learning rule-based systems,” in Proc. The International Joint Conference on Neural Networks, 1992, pp.343-348.

[6] KDD Cup1999. Intrusion detection systems. [Online]. Available: http://kdd.ics.uci.edu /databases/kddcup99/kddcup99.html

[7] J. Sharma and S. Mehta, “Training of radial basis function using particle swarm optimization,” International Journal of Engineering Research and Development, vol. 7, issue 10, pp. 1-10, July 2013.

[8] S. N. Qasem and S. M. H. Shamsuddin, “Improving generalization of radial basis function network with adaptive multi-objective particleswarmoptimization,”inProc.the2009IEEE InternationalConferenceon Systems, Man, and Cybernetics San Antonio, October 2009.

[9] A.Abraham and R. Jain, “Soft Computing models for network intrusion detection systems,” USA, 2006.

[10] R. Agrawa, H. Mannila, R. Srikant, H. Toivonen, and I. Verkamo,“Fast discovery of association

rules," Advances in Knowledge Discovery and Data Mining, AAAI Press/The MIT Press, CA, 1996, Pp.307-328.