International Journal of Engineering & Technology, 7 (4.36) (2018) 557-561

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Efficient Ids Based on Fuzzy Firefly Optimization and Fast Learning Network

Bh.Dasaradha Ram[1*], B.V. Subba Rao[2]

[1]Research Scholar, Department of CSE, Rayalaseema University, Kurnool, AP, India.
[2]Professor, Head of the Department, Department of IT, PVP Siddhartha Engineering College, Vijayawada, AP, India.
**Corresponding author E-mail:bhdasaradh@gmail.com*

Abstract

Overseen Interruption Recognition Framework is a framework that has the capacity of picking up from cases about past attacks to perceive new strikes. Using ANN based interruption discovery is promising for decreasing the amount of false negative or false positives in light of the fact that ANN has the capacity of picking up from certified cases. In this article, a made learning model for Quick Learning System (FLN) in light of fluffy firefly streamlining (FFO) has been proposed and named as FF-FLN. The model has been associated with the issue of interruption location and endorsed in perspective of the famous dataset KDD99. Our created strategy has been taken a gander at against a broad assortment of meta-heuristic figurings for planning ELM, and FLN classifier. FF-FLN has defeated other learning approaches in the testing exactness of the learning.

Keywords: *Fast learning network, IDS, Fuzzy Firefly's, ANN.*

1. Introduction

In current days, security angles for PC arrange is a key disturb of PC human advancement in view of the quick improvement of advances and web administrations. Advances in PC innovation have engaged a few new possibilities, including the capacity to remotely control and oversee frameworks, too opening up a door to get together of data through online sources. In associations level the essential concern is digital security, it investigated the different issues experienced by Multinational organizations in watch their data security, accessibility and unwavering quality. The inspiration has made by above thing for keeping frameworks anchored from any fringe machines, program, or individual going for breaking the security line of the system. There are numerous trappings and applications innovatively progressed to development the security of the environment like machines, systems and PCs. There is a one instrument that endeavors to shield the machines from an aggressor is called Interruption identification framework (IDS).IDS screens the single machine or PC compose for interloper [2]. It is useful in perceiving successful intrusions, and in addition in watching tries to break security, which gives basic information to favorable counter-measures [3].
The basic recommendation to use interruption identification endeavoring to address misuses and frameworks organization attacks in PCs, was progressed by Dorothy E. Denning in 1987 [4]. The strategy is executed by an interruption identification system. Before long such systems are for the most part available with combination. [5], points out the general deficiency and nonattendance of ampleness gave by the present monetarily open structures, this uncovered the necessity for advancing exploration on more intense interruption identification systems. With a particular ultimate objective to execute the methodology of interruption location, there is a need to recognize constant or attempted interruptions or strikes on the structure or framework, this unmistakable evidence data consolidate data aggregation, lead portrayal, data decreasing, and in end declaring and response, this is suggested, as ID [6].The IDS tried to choose whenever checked customer activity or framework development is threatening. If a noxious attack is distinguished, an alert would be made. Diverse particular are available for IDSs' to perceive an ambush, for instance, eccentricity discovery or signs of attack, [7] moreover raises that the accomplishment of IDS depends on these systems. One among the first factors speaking to the ampleness of the IDS is the idea of the component advancement and feature assurance figuring.
There exists an extensive number of procedures, a vast segment of which have been used for different interruption location models to play out a varying arrangement of basic errands, a segment of these techniques fuse; Machine learning based, Half and half ANN based and also planned frameworks. Likewise, as shown by [8], there are cream data mining designs, different leveled hybrid keen structure models, and outfit learning approaches all of which have gotten popularity in progress investigated.
In this paper we proposed an IDS dependent on Quick learning system and an advanced strategy called Fluffy firefly technique. Whatever remains of the present work is organized everything considered.

2. Related work

In The likelihood of an execution examination among Grunt and Suricata isn't new. Both perform well, anyway are not perfect and have confinements as showed up in our examinations. Snort has a lone hung outline, and Suricata has a multi-hung designing which makes the two IDS obvious from one another, yet the oversee set is the customary part of the two IDS. Gathering the framework development and accuracy of the control set are the key parts of the two IDS's execution. In addition, PC have execution unmistakably influences the general IDS execution. An execution examination consider [8] was finished on Grunt and Suricata IDS

and the tests were performed to discover PC have resource utilize execution and ID exactness.

The examinations were performed on two differing PC has with different CPU, 4 memory and framework card particulars. Their results showed that Suricata required a higher taking care of ability to work honorably generally when appeared differently in relation to Grunt. Furthermore, the results exhibited that with higher planning power Suricata could correctly distinguish malignant development on the framework and its lead set was effective [8]. Later in 2013, the definitive appraisal of three IDSs by Wang et al. deduced that Grunt utilized low enrolling resources and its manage set definitely portrayed the true blue and harmful framework action. The pros evaluated the execution of three IDSs in a repeated area. The earth involved physical and virtual PCs. The examination occurs showed that Grunt could contrarily influence organize development more than the other two attempted IDSs [9]. Bulajoul et al. [10] created a bona fide framework to do the examinations that used Grunt IDS. This examination showed the nonattendance of limit of Grunt IDS to process different groups at quick and it dropped packages without correctly separating them. The examination contemplated that Grunt IDS fail to process quick framework movement and the package drop rate was higher. The investigators familiar a parallel IDS advancement with decrease the package drop rate as an answer. (Waleed, Anne and Mandeep, 2013). The execution of Grunt IDS was upgraded by using dynamic development care histograms.

This examination discusses the best strategy to use the demand of ambush signature oversees and moreover the demand of the lead field. The proposed methodology uses the histograms for predicting the accompanying imprint standards and oversee field orders. The multiplication performed exhibited that the proposed methodology basically upgraded Grunt execution [11]. Saboor et al. evaluated the Grunt execution against DDoS. The evaluation rationality involved three particular gear plans. The Grunt execution was viewed the extent that package dealing with and acknowledgment precision against DDoS on three particular hardware plans. The preliminaries occurs exhibited that Grunt package dealing with could be improved by using better hardware outlines, yet Grunt acknowledgment capacity was not upgraded by using better gear [12].

Shahbaz, et al. [13] on the adequacy change of IDS, addresses the issue of dimensionality decreasing by proposing a capable segment assurance count that ponders the association between's a subset of features and the lead class name. Alhomoud et al. [14] have attempted and analyzed the execution of Grunt and Suricata. Both were executed on three particular stages (ESXi virtual server, Linux 2.6 and FreeBSD). The development speed of up to 2 Gbps was used as a piece of this paper. Albin [15] considered the execution of two open-source interference distinguishing proof structures, Grunt and Suricata, by evaluating the speed, memory necessities, and precision of the area engines in an arrangement of preliminaries.

Zammit [16] executed an interference recognizable proof structure that uses machine learning procedures to portray development made from honeypot affiliations. Huang et al. [17] analyzed and executed the Grunt interference area show in a grounds mastermind. Victor et al. [18] endeavored to design an operational model for minimization of false positive IDS alarms, including rehashing alerts by the security executive. White et al. [19] presents a concentrated examination of the execution of Grunt and Suricata. They investigate the execution of the two systems as they scale structure resources, for instance, the amount of CPU focuses, the oversee sets used and the outstanding burdens took care of.

There are diverse works that looks the interference recognizable proof capacity as in [20], tweaking IDS execution as in [21], parallel arrangement of IDS on many-focus processors as in [22], a methodology for restricting together run based significant bundle appraisal as in [23], a Superior Grunt Interruption Identification/Avoidance Framework (BSnort) that usages Aho-Corasick robot as in [24], improving the exactness of framework intrusion acknowledgment systems as in [25], boosting throughput of Grunt NIDS under Linux as in [26], evaluation examinations of three IDS under various attacks and control sets as in [27] et cetera.

3. Proposed model

This territory shows the made framework for this investigation. Immediately, fluffy based firefly change is FFA shown in region. Moreover, Quick Learning System (FLN) displayed in territory. Thirdly, our adaption of FFA to collect FLN based getting ready for IDS is presented in region. In this examination, another FFA is proposed. In the standard FA, in each cycle the more splendid firefly (neighborhood optima) applies its effect over various fireflies and pulls in them toward itself in growth change. As a matter of fact, in the standard FA, fireflies move paying little notice to the overall optima, which can grow the amount of emphasess to find the overall best and decreasing examination of the firefly count. In this examination, to get rid of the weaknesses of the standard FA and to upgrade the total improvement of fireflies, we propose a fluffy based changed variation of FA in which a couple of fireflies in each cycle can affect others and their advancements.

It should be indicated that, in the standard FA, only a solitary firefly in each cycle can impact others and draw in its neighbors.

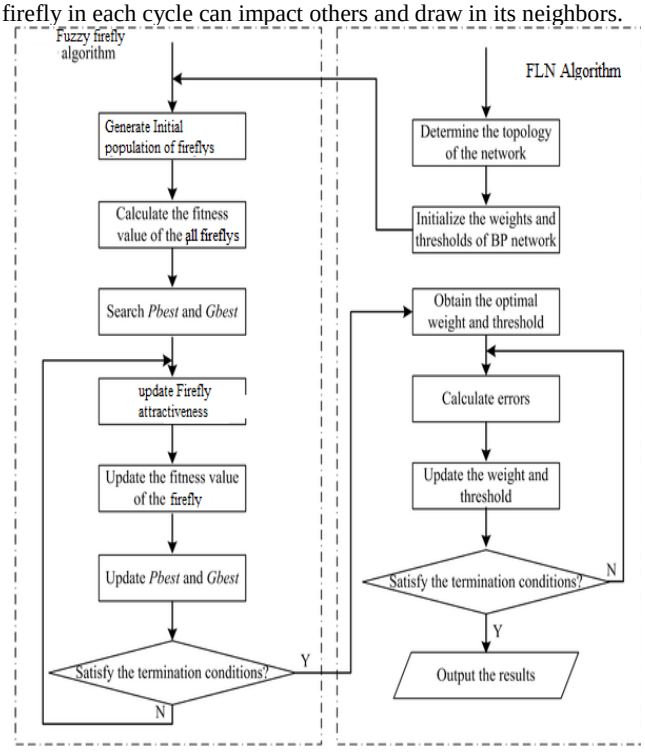

Figure 1: proposed model of FF-FLN

The appeal of each firefly depends upon its magnificence. The level of appeal of each k-best firefly is addressed as a fluffy variable. In the proposed computation, the k-more brilliant fireflies in each cycle are been contenders, where k is a customer set parameter and it depends upon the versatile quality and the people size of the issue. The amounts of alternatives are plausible for the connecting with quality support work. In this examination, we use the Cauchy fill in as an enlistment limit of the proposed calculation.Figure-1 exhibits the fluffy firefly based brisk learning framework for IDS.Let h be one of the k-more splendid fireflies in each cycle, and f (qg) insinuates the health of the area optima (a firefly that is more splendid than the took a gander at one) in each accentuation. We enroll the appeal A(n) of firefly n as

where f(qn) is the health limit of k-more brilliant fireflies. To keep up a vital separation from dependence on the measure of the health work, we set

$$A(n) = \frac{1}{\left(\frac{f(q_n) - f(q_g)}{B}\right)}$$

$$B = \frac{f(q_g)}{s}$$

$$X_i = x_i + \left(B_0 e^{-c r_{ij}^2}(x_j - x_i) + \sum_{h=1}^{k} A(n) B_0 e^{-c r_{in}^2}(x_n - x_i)\right) \alpha \left(\text{ran}\right.$$

where s is a customer decided parameter. For a settled f(qn), the greater the estimation of s, the smaller the drawing in quality A(n). In the FFA, we use Cartesian detachment to process the partition of yet for advancement of the firefly,
Where xi is the spatial sort out of the less mind blowing firefly, second term is a direct result of the interest of the more brilliant firefly, and the third term is a fluffy variable that shows the level of charm of k-more brilliant fireflies (in all n fireflies) in the improvement of fireflies.

3.1. Fast learning network

The Quick Learning System (FLN), proposed by [15], is a parallel relationship of a SLFN and a 3 layer FNN: input, covered and yield layer. FLN, a Fake Neural System, or, in other words Parallel Forward Neural System (DPFNN), is appeared underneath utilizing an illustrative methodology, particularly the scarcest square's frameworks as appeared in Fig. 1

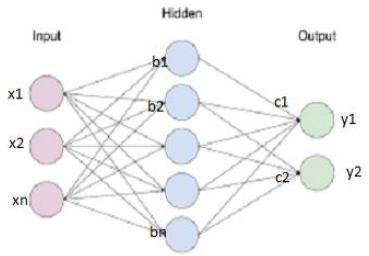

Figure 2: Structure of the FLN

The FLN is fundamentally a DPFNN. T
The FLN is mathematically modeled as [15]:

$$Y = f(w^{io}x + w^{oh}G + c) = f\left([w^{io}w^{oh}c]\begin{bmatrix}X\\G\\I\end{bmatrix}\right) =$$

$$f\begin{pmatrix} w & \begin{matrix}X\\G\\I\end{matrix}\end{pmatrix}$$

$$\boldsymbol{G}\,(w^{in}, \ldots, w_m{}^{in}, b1 \ldots, bm, X1, \ldots, XN)$$

$$= \begin{bmatrix} g(w_1^{in}x_1 + b_1) & \cdots & g(w_1^{in}x_N + b_1) \\ \vdots & \ddots & \vdots \\ g(w_m^{in}x_1 + b_m) & \cdots & g(w_m^{in}x_N + b_m) \end{bmatrix}_{m\times N}$$

$$W = [w^{io}w^{oh}c]_{i\times(n+m+1)}$$

$$W = [wiowohc]\times(n+m+1)$$

$$I = [11 \ldots \ldots \ldots 1]\times N$$

Where N addresses the amount of specific precedents in $\{xi, yi\}$, in which is the n-dimensional tuft vector of the I-th test,

likewise, $yi = [yi\ 1\ ,\ yi\ 2, \ldots\ ,\ yil]T \in Rl$ is the contrasting l -dimensional yield vector.

m addresses the amount of covered layer centers. win is the m × n input weight framework,

b = ($b1$, $b2$, … ,) addresses the inclinations of the covered layer center points, and woh is a $l \times m$ organize which contains the weight estimations of the interfacing between the yield layer and the data layer,

C = [$c1$, $c2$, … , ci]T is the inclinations of yield layer centers.

g(.) and f(.) address the dynamic components of the covered centers and yield centers independently.,

woi= [$w1oi$, $w2$, … . $wioi$] addresses the weight vector associating the jth yield center point and the information centers,
$wkok$= [$w1koh$, $w2koh$, … . $wikoh$] is the weight vector interfacing the kth covered center point and the yield center points,
additionally, $wkin$ = [$wk1in$, $wk2in$, … ., $wkmin$]T is the weight vector associating the kth hid center point and the data center points.
The structure W= [$\mathbf{W}oi\mathbf{W}oh\mathbf{c}$] could be called as yield weights.
G is seen as the covered layer yield framework of FLN.
As imparted in the issue assertion, FLN takes after ELM with respect to lacking flawless weights, stream or errand. Similarly, the general exactness of the ANN will be defiled beside if a reasonable course with a specific genuine goal to pick the weights is performed. Our Firefly-Based enhanced FLN is set up in light of picking weights utilizing firefly streamlining. Firefly-constructed progression of FLN depends with respect to arranging a firefly that addresses one candidate course of action of FLN weights. One specific issue in playing out the change is requiring to pick both the weight's characteristics and moreover the amount of neurons that are required in the disguised layer of accomplish better accuracy. This infers a variable length through the course of action as demonstrated by the amount of the hid neurons in FLN, and to crush this issue, the best number of neurons in considered in doling out a length for the atom. For commencement work, tanging has been used for the yield of the disguised layer neurons.
y=(x)=2/1+e−2x−1 where x∈[−1,1]

By using this limit, we can cover the case of counterbalancing the neurons of the covered layer orchestrate when the weights are been zeros. In the going with, the pseudo-code of Firefly - based progression is showed up.
Step-1: Create Preliminary Group of firefly's. $Pi = \{wj\}$, i = 1…N
J= 1, …M, N residents size, M weights number
Step-2: For each firefly do the subsequent
Step-2.1: For each firefly build an corresponding FLN system.
Step-3: For each FLN ensure the subsequent
Step-3.1: Compute accurateness of the FLN
Step-3.2: If the capability value is better than the best local capability value (pLBest) in antiquity
Step-3.2.1:Fixedup-to-date value as the fresh pLBest
Step-3.2.2: End If
Step-3.3: If the capability value is superior than the finest overall capability value (pLBest) set current
Step-10: Worth as the fresh pLBest
Step-3.4: Update firefly spot rendering to the spot equation
Step-3.5: Go to Step-3
The methodology proposed in this paper is for planning ANN as a way to deal with update the execution of IDS for better strike gathering process. This is expert by methods for the fluffy based firefly to crush the issues that commonly are looked by the machine learning strategies like; entrapment in adjacent minima, association speed, and affectability to instatement. In any case, we segment the dataset into two data sections for getting ready 80% and testing 20%. By then, we develop a standard dataset plan with the ultimate objective of redoing by ANN. As needs be, the point at which the readiness of the ANN has finished, the ANN starts its method in portraying the KDD Glass '99 testing dataset and takes the exact yields of the IDS's recognition. By then, every one of these methods are recorded and checked as a way to deal with improve the framework after n emphasess. Exactly when the affirmation time of the ANN is done, at that stage, the ANN patching up would be tried to be streamlined by our proposed Fluffy firefly estimation. Right when the delayed consequences of the ANN are enhanced by our proposed fluffy firefly FLN figuring, they will be differentiated and GA-Based ELM PSO-

Based ELM Essential FLN GA-Based FLN PSO-Based FLN the ANN be more inquired about in the ANN patching up in the field of IDS with the KDD Container dataset. To help ANN in IDS streamlining, the fluffy firefly is realized in this paper. Fluffy based firefly is used as a piece of this paper with FLN to help ANN in the midst of IDS's attack affirmation process.

4. Experimental data

ANN based intrusion distinguishing proof must be set up on picked Dataset. With a particular ultimate objective to display the feasibility of our model, we pick the most critical dataset in regards to reference to the composition of interference KD99. Additionally, we present the particular issue that is tended to in the composition.

Diagram of KDD informational collection:

KDD Glass 99 is seen as the most recognized research dataset exceedingly reasonable to benchmark execution [17], moreover observes its usage in differentiating the suitability of various procedures with System Interruption. KDD Container 99 is produced in perspective of the data got in DARPA'98 IDS program [18]. DARPA'98 contains about 4GB of compacted unrefined (twofold) tcpdump data. This contains around 7 weeks of checked framework movement. This data can in this way, be directed into around 5 million associating records, each around 100 bytes. KDD planning instructive accumulation involves around 4,900,000 single affiliation vectors each one of which contains 41 incorporates and is set apart as either customary or a strike, [19], the attacks can starting there be requested into correctly one of four, as bare essential underneath;

Foreswearing Administration of Assault (DoS):

This assault incorporates every one of the assets and make them occupied and make the assets does not ready to deal with some other solicitations. The attacker making usage of specific advantages for a degree that denied access for true blue customers. Client to Root Assault (U2R): It is a kind of security misuse, whereby the attacker would get to a common customer account, through standard means, and starting there keep on trying root access to the system through the abuse of a defenselessness.

Remote to Neighborhood Assault (R2L): this is the time when an attacker attempts access to a structure over a framework. The attacker can simply transmit data packages over the framework, the assailant tries to get to the machine, by abusing some shortcoming.

Testing Assault (Prob): It is the time when an aggressor tries to acquire information from a framework, for evading the systems, security traditions.

Since 1999, a broad number of examiners reviewed their IDS models using KDD Glass 99. This shows how KDD Container 99 has been a working benchmark enlightening file for over 15 years, is still successfully open and available today.

The objective of the KDD 99 IDS competition is to make a standard instructive gathering for the investigating and appraisal of research in intrusion recognizable proof, [15]. Authorities found a couple of difficulties or obstructions in getting ready with KDD99, Olusola et al. [16] have analyzed the KDD 99 enlightening list for picking a relevant segment. They proposed that a couple of features or attributes were not related to any attack, [17] they have taken 10% of the whole instructive accumulation to play out their examination.

5. Experimental setup

5.1.Data set

Keeping in mind the end goal to fabricate a compelling and dependable ANN based interruption recognition framework, there is a high need to give far reaching data set to instructing the ANN show. Albeit a few data sets exist inside the writing for such an information working, there is a critical test that should be tended to in this regard. All the more particularly, the vast majority of the dataset don't give enough cases to instructing the models in an express route because of the less recurrence of a few assaults. This has made a worry on how depend on the accessible little cases of data of assaults so as to construct generalizable learning for AI models to utilize it in distinguishing comparable non-put away assaults. A case for one normal dataset utilized for preparing models on interruption assaults is KDD99.

Experimental toolkit: Here we use Anaconda-3 integrated development tool and an editor called spyder is used for implementing the code. Python programming language is used develop this model and Python matplot package is used to generate the graphs. For to develop Intel core-3 processor and 4GB Ram and 1TB HDD is used for simulations and the OS is Windows-8.

6. Results and discussions

Here below table shows the comparison of our proposed fuzzy firefly FLN algorithm, with GA-Based ELM PSO-Based ELM Basic FLN GA-Based FLN PSO-Based FLN the ANN be more researched in the ANN rearrangement in the field of IDS with the KDD CUP dataset. To help ANN in IDS advancement, the fuzzy firefly is executed in this paper. Fuzzy based firefly is utilized as a part of this paper with FLN to help ANN amid IDS's assault acknowledgment process.

Table 1: Comparison of Proposed Fuzzy Firefly FLN Algorithm with Existing Methods

Number of neurons in the hidden layer	30	60	90	120	150	180	210	240
GA-Based ELM	0.9834	0.9873	0.988	0.9894	0.9909	0.9909	0.9924	0.9947
PSO-Based ELM	0.9815	0.9867	0.9859	0.99	0.9904	0.9921	0.9923	0.9951
Basic FLN	0.9868	0.9889	0.9901	0.9912	0.9923	0.9932	0.9956	0.9957
GA-Based FLN	0.9885	0.9899	0.9904	0.9917	0.992	0.9926	0.9956	0.9969
PSO-Based FLN	0.9892	0.9895	0.9904	0.9907	0.9919	0.9927	0.9935	0.9968
Firefly based FLN	0.9898	0.9912	0.9921	0.9930	0.9942	0.9947	0.9972	0.9982

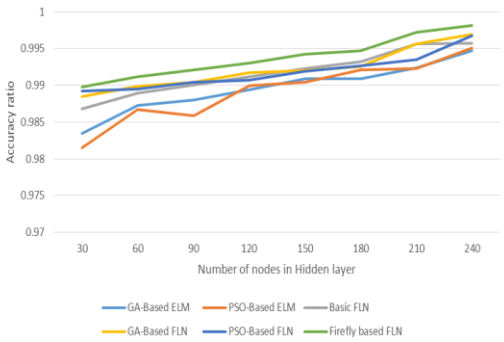

Figure-3: accuracy of different optimization approaches with respect to the number of neurons

Figure-3 shows the comparison of accuracy of different IDS algorithms by varying the number of hidden nodes in fast learning network. The proposed FF-FLN gives better accurate results than all other.

7. Conclusion

In this paper, we handled the issue of IDS. For that we used ANN based IDS is also promising for diminishing the amount of incorrectbad or erroneous great because ANN has the capacity of picking up from genuine outlines. A made learning prototypical for FLN in perspective of soft firefly upgrade has been foreseen and named as FF-FLN. The prototypical has been associated with the issue of IDS and affirmed in light of the notable dataset KDD99. Our made show has been considered against the broad assortment of meta-heuristic figurings for planning ELM, and FLN classifier. It tends to be surmised that our made FF-FLN has beated previous learning strategies in the testing precision of the learning. Another finding is that the accuracy has extended for all models with growing the amount of covered neurons in the ANN Future work is to counter the issue of less precision for a particular number of class because of the limited available proportion of getting ready data for such class.

References

[1] Eberhart RC &Kennedy J, "A new optimizer using particles swarm theory", *Sixth Int. Symp. on Micro Machine and Human Science*, (1995), pp.39–43.

[2] Eberhart RC & Kennedy J, "Particle swarm optimization", *IEEE Int. Conf. on Neural Network*, (1995), pp.1942–1948.

[3] Shi Y & Eberhart RC, "A modified particle swarm optimizer", *IEEE World Conf. on Computation Intelligence*, (1998), pp.69–73.

[4] Shi Y & Eberhart RC, "Empirical study of Particle Swarm Optimization", *IEEE World Conference on Evolutionary Computation*, (1999), pp.6–9.

[5] Yao X, "A review of evolutionary artificial neural networks", *Int. J. Intell. Syst.*, Vol.8, No.4, (1993), pp.539–567.

[6] Angeline PJ, Sauders GM & Pollack JB, "An evolutionary algorithm that constructs recurrent neural networks", *IEEE Trans. Neural Networks*, Vol.5, No.1, (1994), pp.54–65.

[7] Marco G & Alberto T, "On the problem of local minima in back-propagation", *IEEE Trans. Pattern Anal. Mach. Intell.*, Vol.14, No.1, (1992), pp.76–86.

[8] Van Ooyen A & Nienhuis B, "Improving the convergence of the back-propagation algorithm", *Neural Network*, Vol.5, No.4, (1992), pp.465–471.

[9] Ahmad M & Salam FMA, "Supervised learning using the Cauchy energy function", *International Conference ON Fuzzy logic and Neural Networks*, (1992), pp.721-724.

[10] Jacobs RA, "Increased rates of convergence through learning rate adaptation", *Neural Networks*, Vol.1, (1988), pp.295–307.

[11] Weirs MK, "A method for self-determination of adaptive learning rates in back propagation", *Neural Networks*, Vol.4, (1991), pp.371–379.

[12] Irie B & Miyake S, "Capability of three-layered perceptron", *IEEE Int. Conf. On Neural Networks*, (1998), pp.641–648.

[13] Shaw S & Kinsner W, "Chaotic simulated annealing in multilayer feed forward networks", *In Canadian Conf. on Electrical and Computer Engineering*, Vol. 1, (1996), pp.265–269.

[14] Seop KC, Mohammed OA & Song YH, "Detection of magnetic body using article neural network with modified simulated annealing", *IEEE Trans. Magn.*, Vol.30, (1994), pp.3644–3647.

[15] Bhattacharya U & Parui SK, "The Use of Self-adaptive learning rates to improve the convergence of backpropagation algorithm", *Tech. Rep. GVPR-1/95, CVPR Unit, Indian Statistical Institute, Calcutta, India*, (1995).

[16] Chunkai Z, Huihe S & Yu L, "Particle swarm optimization for evolving artificial neural network", *IEEE Int. Conf. on System, Man, and Cybernetics*, Vol.4, (2000), pp.2487–2490.

[17] Shi YH & Eberhart RC, "Parameter selection in particle swarm optimization", *Annual conference on Evolutionary Programming*, (1998), pp.591-600.

[18] Salerno J, "Using the particle swarm optimization technique to train a recurrent neural model", *Ninth IEEE Int. Conf. on Tools with Artificial Intelligence*, (1997), pp.45–49.

[19] Eberhart RC & Shi Y, "Comparing Inertia Weights and Constriction Factors in Particle swarm Optimization", *Proc. of congress on Evolutionary Computing*, Vol.1, (2000), pp.84–88.

[20] Homik K, "Multilayer feed forward networks are universal approximators", *Neural Networks*, Vol.2, (1989), pp.359–366.

[21] Boeringer DW & Werner DH, "Particle swarm optimization versus genetic algorithms for phased array synthesis", *IEEE Trans. Antennas Propagation*, Vol.52, No.3, (2004), pp.771–779.