Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 7, No. 3, September 2019, pp.1067-1073
Available online at: *http://pen.ius.edu.ba*

Review of neural networks and particle swarm optimization contribution in intrusion detection

Maha Mahmood[1] and Belal Al-Khateeb[2]

[1]**College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq**

[2]**College of Computer Science and Information Technology, University of Anbar, Ramadi, Iraq**

Article Info

Feb 03, 2019

Keyword:

Intrusion Detection
Neural Network
Particle Swarm Optimization
Algorithm, Machine
Learning.Reconstruction

ABSTRACT

The progress in the field of computer networks and internet is increasing with tremendous volume in recent years. This raises important issues concerning security. Several solutions emerged in the past, which provide security at the host or network level. These traditional solutions like antivirus, firewall, spyware and authentication mechanism provide security to some extents but they still face the challenges of inherent system flaws and social engineering attacks. Some interesting solution emerged like intrusion detection and prevention systems but these too have some problems like detecting and responding in real time and discovering novel attacks. Because the network intrusion behaviors are characterized with uncertainty, complexity and diversity, an intrusion detection method based on neural network and Particle Swarm Optimization (PSO) algorithm is widely used in order to address the problem. This paper gives an insight into how PSO and its variants can be combined with various neural network techniques in order to be used for anomaly detection in network intrusion detection system in order to enhance the performance of intrusion detection system.

Corresponding Author:

Maha Mahmood,
Computer Science,
College of Computer Science and Information Technology, University of Anbar

Email: maha_mahmood@computer-college.org

1. Introduction

There are some significant problems in the Intrusion Detection System (IDS), such as big load, slow detection speed and large amount of data. IDS is unable to deal with those problems in a real time. In large or small networks, there are very large network traffic data quantities that need to be examined by IDS. Detecting speed represents one of the most important indexes of IDS real time requirements. With the IDS continuous network technology development, the intrusion behaviors can be characterized with diversity, dynamic tendency, complexity and uncertainty. Network intrusion detection is a dynamic protection technology that is based on the self-defense of the web [1]. It can effectively deal with the external networks attacks and more importantly, it is able to prevent the violations from internal networks, this makes the intrusion detection technologies able to detect the known and unknown intrusions effectively and in good time speed. Recently,

artificial intelligence techniques are used in intrusion detection in order to improve the detection accuracy. Neural networks are one of the most effective artificial intelligence methods that are employed in IDS [2]. A combination of IDS and neural network algorithm (self-learning and adaptive ability) is used to improve the IDS performance [3], [4]. Artificial Neural Network (ANN) is used for IDS pattern analysis. Many parameters can affect the ANN classification quality, like determining the architecture, over fitting and local minima. In addition, many irrelevant variables in the real intrusion detection sample data affect the ANN classification quality, decrease the real time capacity and increase many unwanted calculations for the intrusion detection. A good and feasible option is to use the features reduction methods like the principle component analysis [5]. Those features reduction methods usually lose useful information. Therefore, PSO algorithm is one of the possible solutions.

PSO algorithm is an optimum algorithm is one of the random optimizing process methods [6], that has some advantages such as high efficiency, parallel search and able to overcome the problem of local convergence. PSO is able to find a near to global optimal solution in a short time [7].

2. Neural Networks and Particle Swarm Optimization Algorithm

Neural Network (NN) is one of the machine learning algorithms that maps inputs to outputs through input and output membership functions together with an associated parameter. NN is able to handle complex nonlinear systems data without the need for identifying the nonlinear associations between inputs and outputs through a physical/logical model. Back Propagation Neural Network (BPNN) represents one of the most popular neural networks that is extensively used to characterize nonlinear systems but in fact, it is not suitable for noisy real world applications as it suffers from the network initial weights high sensitivity, local optima convergence and low rate convergence. The initial values of the weights particularly have a great influence on the accuracy and convergence of NN [3]. Therefore, many methods, like the momentum algorithm, have been presented to improve the NN performance [3]. PSO algorithm is proposed as a way to refine NNs the weights initialization effect reduction and for overcoming the slow convergence limitations. Similar to the biological neural cell, the neuron represents the unit of structure of ANN, basically each neuron consists of a summer and an activation function, the structure of an artificial neuron is shown in fig. (1) [12].

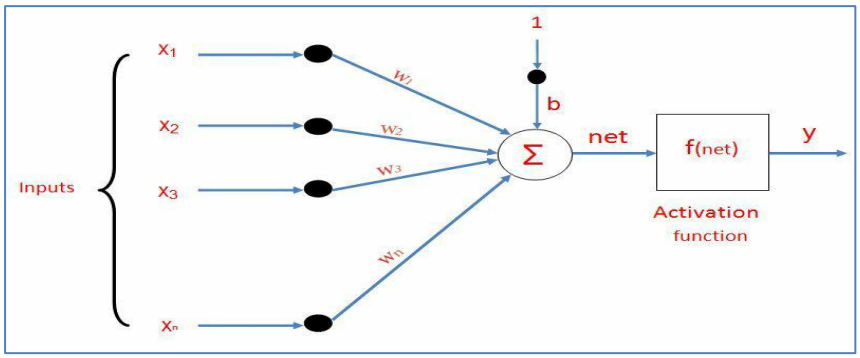

Fig (1): Structure of the Artificial Neuron.

In figure 1, the x1, x2, x3…, xn. represent the neuron inputs with corresponding weights w1, w2, w3…, wn. that simulates the biological nets neural connections. Sometimes, a threshold term b is added to the inputs [12] Where f is called the neuron activation function or the neuron transfer function Output could be bipolar, binary or real value. In order to form the net input to the neuron (net), the inputs are multiplied by their corresponding weights and then added together. This is done by:

$$\text{Net} = \sum_{i=1}^{n} wixi + b = w_1x_1 + w_2x_2 + w_3x_3 + \ldots\ldots + w_nx_n + b \qquad (1)$$

In order to produce an output Y, the neuron represents the activation or mapping function f(net), is calculated as follows [3].

$$Y = f(net) = f\ \sum_{i=1}^{n} wixi + b \qquad (2)$$

There are a number of types of commonly used activation functions. Most activation functions are also known as threshold functions.

Particle Swarm Optimization (PSO) algorithm is proposed by Kennedy and Eberhart in 1995 [8]. The foundation of PSO is based on simulating behaviour of animals that are working in groups such as birds and fishes [9]. In PSO algorithm, many creatures, are called particles, are distributed in the search space that belongs to the function that is required to be optimized. The objective function value is calculated by each particle according to its position that can be set according to its best previous position and according to its neighbour's best previous position [10]. The calculation of the objective function and the position are repeated several times until it converged to the desired goal. PSO algorithm is characterized by its simplicity and ability to converge to good result, which make the algorithm popular [11]. In PSO, the problem is analyzed by exchanging information between the particles [11], and random positions and velocities are used to make the particles. The following equations are used to update each particle position and velocity, in the current step of the algorithm:

$$V_{i,j}(t+1) = wV_{i,j}(t) + r_1c_1\left[Pbest_{i,j}(t) - X_{i,j}(t)\right] + r_2c_2\left[Gbest(t) - X_{i,j}(t)\right] \qquad (3)$$

$$X_{i,j}(t+1) = X_{i,j}(t) + V_{i,j}(t+1) \qquad (4)$$

where $\boldsymbol{V}$ is a velocity of $\boldsymbol{i}$ particle at iteration $\boldsymbol{t}$; $\boldsymbol{X}$ is a position of particle $\boldsymbol{i}$ at iteration $\boldsymbol{t}$ and it depends on previous position and new velocity, $\boldsymbol{w}$ is the inertia weight that is used to control the influence of the previous velocities on the current velocity and $\boldsymbol{c1,c2}$ are two random numbers between (0,1) that represents the learning factors or acceleration factors that are fixed numbers, ***Pbest*** is the local best particle $\boldsymbol{i}$ that have the smallest fitness value obtained so far in one iteration $\boldsymbol{t}$; ***Gbest*** is the particle leader or global best position at generation $\boldsymbol{t}$.

3. Network Intrusion Detection Model

An Intrusion Detection System (IDS), can be hardware or software application, is used to monitor a system or network for policy violations or malicious activity. Security Information and Event Management (SIEM) system is used to typically collect centrally any violation or malicious activity. Those violations and malicious activity can also be reported to an administrator. A SIEM system combined the outputs that are collected from multiple sources then distinguishes malicious activity from false alarms by using alarm filtering techniques [13]. There many types of IDS that are ranging from single computers to large networks. Network Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS) represent the most common classifications. An example of NIDS is a system that analyzes incoming network traffic while monitoring important operating system files represents HIDS example. IDS can be also classified by detection approach, those can be divided into anomaly based detection (detecting deviations from a model of "good" traffic, which often used machine learning) and signature based detection (recognizing bad patterns, such as malware) [14], [18]. Some IDS products are called an intrusion prevention system as they have the ability of responding to the detected intrusions [15].

4. Literature Review

Zhiwei Wang, Gregory L. Durst, Eli Lilly and Zina Ben-Miled [21], re-established the results of feature selection using binary PSO in the first round and using a back propagation neural network to generate the Quantitative Structure Activity Relationship (QSAR) model in the second round, the features that are selected in the first round are used in the QSAR generation. A new method that overcomes the back propagation limitations is then proposed. In the new approach, PSO is used in the second round for training and

overcoming the instability of PSO by bootstrap aggregation (Bagging). Robust QSAR models are produced by the proposed approach; also, the variability is reduced due to the back propagation parameters choice.

WenJie Tian and Ji Cheng Liu [16], constructed the structure of the network and gave the flow of algorithm, which analyzed and discussed the intrusion behaviours impact factor. With the faster convergence and strong self-learning ability, the proposed method can rapidly detect many intrusion behaviours in an effective way by the typical intrusion characteristic information learning. The proposed method reduced (without losing ability) the full dataset and used it to train the neural network, which increased the detection accuracy. The experimental results on KDD99 dataset show the feasible and effective ability of the proposed anomaly intrusion detection method as it has the ability to determine whether there is an intrusion information or not. The proposed method can truly detect the anomaly intrusion behaviour, this is done by the ability of function approach, fast convergence rate and strong self-learning. Both simulations and experiments showed how the proposed method is extremely ubiquitous and effective, this indicates the great application of the proposed method in the network security.

Diptam Dutta and Kaustav Choudhuryusing [5], presented a novel monitoring of Simple Network Management Protocol (SNMP). The proposed method combined PSO and neural network training with the Digital Signature of Network Segment (DSNS). The SVM is used by the proposed anomaly detection system for traffic clusterization, SNMP agents and its respective DSNS are used for traffic collection. PSO is combined with the SVM for improving the solution performance and quality in the clusterization and clusters centroids calculation. The designed model is implemented on FPGA (Spartan 3E) in order to use the solutions hardware integration in the areas of diagnosis, monitoring and network intrusions management. The Techno India University, Kolkata real network environment is used to test the proposed method. The obtained results demonstrated that the false alarm and detection rates are good and promising. It is recommended to detect anomalies, using the same dataset, by the proposed method in order to have the ability of comparing both methods.

Kang Xie [8] proposed a new method of hierarchical intrusion detection algorithm based on the Discrete Cellular Neural Networks (HDCNN) in order to solve the problems of low accuracy and slow speed in the existing intrusion detection algorithms. In order to obtain the template parameters for the HDCNN classifier, energy function constraint method is used to construct a new PSO fitness function, jumping out the premature convergence. Emerging evidence has indicated that this new approach is affordable to parallelism and analog VLSI implementation. Experimental results and comparative studies based on the KDDCUP99 data sets are given, show that the proposed model exhibits an excellent performance owing to the higher attack detection rate and shorter processing time.

Matthew L Settles and Bart Rylander [11], employed PSO in a split architecture injected with a plain ‘attractor’ configuration. This is achieved by splitting the input vector into two even sub vectors, then each vector will be optimized using its swarm at which a plain ‘attractor’ is injected into each swarm. An investigation of this technique application to neural network training is done. The obtained results indicate that the resulted architecture is promising. Before a conclusion can be reached, a more in depth analysis using another neural nets are needed. It would also be interesting to investigate the performance of the resulted architecture on function minimizations.

Xuesong Wang and Guangzhan Feng [19], conducted a research on the network intrusion detection system based on the modified particle swarm optimization algorithm. Along with the computer network and the computer system application in various fields in the national life continue to expand, the load types and volume of the business is increasing. How to be reasonable in complex application environment of the system resource allocation and task scheduling, for improving the efficiency of computer system and computer network, reduce running cost is a problem to be solved. Under this background, the researchers combined the particle swarm optimization methodology to propose the enhancement countermeasures for the meaningful contemporary networks.

Priyanka Pawar and Damodar Tiwari [13], analyzed program behaviour in intrusion detection using the PSO and Neural Network. The proposed algorithm is evaluated by experiments on KDDCUP99 dataset. The

obtained results are promising as the Neural Network that is optimized using PSO can achieves a low false positive rate and effectively detect intrusive attacks. Training process is easily added to the neural network training data set without any need for changing the existing training samples weights, this is due to the used frequency weighting method where each entry is equal to the occurrences number of system call during the transmission control protocol communication. The appropriate selection of the input parameters through PSO is used to optimize the system output.

Chandrashekhar Azad and Vijay Kumar Jha [4], used PSO and fuzzy min max neural network in order to propose an intrusion detection system. The proposed system is characterized with its online adaption facility and the learning requires less time. The proposed system is tested using a preprocessed KDDCUP99 dataset. In order to test the effectiveness of the system, classification accuracy and error are taken as performance evaluation parameters. The obtained results show that the proposed system performance was very good as compared to the other well-known systems like the multilayer perceptron, MLP classifiers, RBFN classifiers, RBF classifier, SMO, Naïve Bayes, LibSVM, KDD Cup Winner, KDD Cup Runner UP, FMMGA and FMM.

Ahmad Shokouh Saljoughi, Mehrdad Mehvarz and Hamid Mirvaziri [1], used MLP Neural Network and PSO algorithm in order to detect intrusions and attacks. The method was tested using KDDCUP and NSL-KDD datasets. The results showed that the accuracy is improved in detecting intrusions and attacks by unauthorized users. In the proposed model, it is attempted to promote the rate of precision to detect different kinds of attacks. The results obtained from integrating the neural network with the PSO algorithm have been presented. The proposed model is evaluated with KDDCUP99 and NSL-KDD databases. In order to detect different kinds of attacks, the precision rate is promoted in the proposed model. KDDCUP99 and NSL-KDD datasets are used for testing of the proposed model, as the optimal weights is extracted by the optimization of the neural network using the proposed integration. The results of integrating the neural network with the PSO algorithm is presented and showed that the proposed model is better than a simple neural network. Furthermore, the time complexity is reduced by using random weights for the training of the neural network and this training will stop if the PSO optimizer is not able to improve the system precision. The obtained results are analysed using the K-fold method and the selection of a random group. Finally, the function of the system is substantially improved in terms of the precision of detecting attacks faced by the networks and the time complexities reduction.

Mohammed Hasan Ali and Mohamed Fadli Zolkipli [9], used PSO algorithm in order to create an optimal RK-FLN classifier named PSO-RKELM, this was done by obtaining Reduce Kernel FLN (RK-FLN optimal set of initial parameters. The proposed method was compared to four models, including basic FLN, basic ELM, RK-FLN and Reduce Kernel ELM (RK-ELM). The model was tested using KDDCup99 dataset and the obtained results demonstrated accuracy, reliability and effectiveness of the proposed PSORKFLN as a classification algorithm. It worth mentioning here that the accuracy of PSO-RKFLN is better than other models. It is recommended to check this model using different neurons number in order to measure and evaluate the model complexity.

Mohammed Hasan Ali, Alyani Ismail and Mohamad Fadli Zolkipli [10], proposed a developed learning model for fast learning network (FLN) based on PSO. This learning model is called PSO-FLN. The develope model is applied to the intrusion detection problem and is tested using KDD99 dataset. For the purpose of training the extreme learning machine and FLN classifier, the developed model is compared against many Meta heuristic algorithms. The obtained results showed that PSO-FLN is better than other learning approaches in terms of accuracy. Also, the results showed that the accuracy for all models is increased when increasing the ANN hidden neurons number. The ANN based intrusion detection is more promising for reducing the number of false positives or wrong negative as ANN is capable of learning from actual examples. It is recommended to address the low accuracy problem for a certain number of classes because of the limitation of the available amount of training data for such classes.

Xiang Changsheng [17], improved the network intrusion detection effectiveness by proposing a network intrusion detection model that is based on PSO and neural network. Firstly, the features of network intrusion detection are collected, PSO algorithm is effectively used to select the important features by removing the invalid feature. Secondly, build the intrusion detection classifier by Backpropagation neural network. Finally,

KDD99 dataset is used for model performance analyzing. The obtained results showed that the proposed method improved the network intrusion detection accuracy, also the detection speed was very good and is recommended to be applied in the network security. Network intrusion detection results of PSO-BPNN has obvious advantages, those are: the network intrusion detection results are better when PSO algorithm select the features, can more establish ideal network intrusion detection model, but also reduce the training time of the classification, fasten network intrusion detection modeling speed, which can be applied to large-scale network intrusion detection, can detect the operation.

Xiang Yu and Claudio Estevez [20], improved the search efficiency by proposing an adaptive update strategy of particle velocity for MSCLPSO. The aim for each particle is how to balance between the associated objective optimization and Pareto set diverse regions exploration. This can be done by an adaptive determination of either only learning from the same swarm particles or additionally from the difference of elitists' pairs for velocity updating on that dimension, this depends on whether the elitists are simple or complex. Many experiments are done using two objectives and three objectives benchmark optimization problems, each problem has different dimensional complexity. The obtained results showed that the proposed method is significantly improves the performance of MSCLPSO search, also MSCLPSO becomes able to locate the true Pareto front in a quicker way and obtain better distributed non dominated solutions over the entire Pareto front. The proposed strategy achieves a good balance between each single objective optimization and the Pareto set exploration. A possible direction for future work is to investigate a different evolution adaptive strategy of the elitists as differential evolution is not of equal usefulness for the simple and complex dimensions. Many different studies have been employed [22- 25].

5. Conclusions

Intrusion detection represents one of the most important fields of the research in the network security field and represents a new defense technology for the network security. Using PSO algorithm and neural networks makes intrusion detection overcome the traditional Backpropagation algorithm problems such as the low converging speed and local minimum, therefore, it enhanced the detecting accuracy and the converging speed of the system. This paper reviewed the most powerful approaches that are based on the combination of PSO and neural networks.

6. Future work

The results indicate that using PSO and neural networks is promising. Although there is a need for experiments, especially for choosing the right architecture for the neural networks.

References

[1] A. Sh. Saljoughi, M. M. and H. Mirvaziri, "Attacks and Intrusion Detection in Cloud Computing Using Neural Networks and Particle Swarm Optimization Algorithms", Emerging Science Journal, Vol. 1, No. 4, 2017.

[2] B. Al-Khateeb, "The Selection of Particle Swarm Optimization Learning Factors Values in Solving the Multiple Travelling Salesman Problem", Jour of Adv. Research in Dynamical & Control Systems, Vol. 10, No. 7, 2018.

[3] B. Al-Khateeb and M. Mahmood, "A Framework for an Automatic Generation of Neural Networks", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 2, 2013.

[4] Ch. Azad and V. K. Jha, "Fuzzy min–max neural network and particle swarm optimization based intrusion detection system", Springer-Verlag Berlin Heidelberg, Volume 23 Issue 4, April 2017.

[5] D. Dutta and K. Choudhury," Network Anomaly Detection using PSO-ANN", International Journal of Computer Applications, Vol. 77, No.2, 2013.

[6] G. Liu, Z. Yi and Sh. Yang," A hierarchical intrusion detection model based on the PCA neural networks", Neurocomputing, Vol. 70, Issue 7, 1561-1568, DOI: 10.1016/j.neucom. 2006.10.146, 2007.

[7] K. Ahmed, B. Al-Khateeb and M. Mahmood, "Application of chaos discrete particle swarm optimization algorithm on pavement maintenance scheduling problem", Cluster Computing the Journal of Networks, Software Tools and Applications, Cluster Compute DOI 10.1007/s10586-018-2239-3, 2018.

[8] K. Xie," Research of Hierarchical Intrusion Detection Model Based on Discrete Cellular Neural Networks", Journal of Information and Computational Science 10(17):5569-5578, DOI: 10.12733/jics20102446, November 2013.

[9] M. H. Ali, A. Ismail and M. F. Zolkipli, "A new intrusion detection system based on Fast Learning Network and Particle swarm optimization", IEEE Access, DOI: 10.1109/ACCESS.2018.2820092. 2018.

[10] M. H. Ali and M. F. Zolkipli, "Model of Improved a Kernel Fast Learning Network Based on Intrusion Detection System", Springer Nature Switzerland, DOI: 10.1007/978-3-030-00979-3_15, 2018.

[11] M. L Settles and B. Rylander, "Neural Network Learning using Particle Swarm Optimizers", Advances in Information Science and Soft Computing, 2002.

[12] M. Mahmood and B. Al-Khateeb, "Towards an Automatic Generation of Neural Networks", Journal of Theoretical and Applied Information Technology, Vol.95. Issue 23, 2017.

[13] P. Pawar and D. Tiwari, "Intrusion Detection System based on Particle Swarm Optimized Neural Network", International Journal of Digital Application & Contemporary Research, Vol. 4, Issue 11, 2016.

[14] S. Al-Janabi, B. Al-Khateeb and A. J. Abd, "Intelligent Techniques in Cryptanalysis: Review and Future Directions", UHD Journal of Science and Technology, Vol 1, Issue 1, 2017.

[15] S. Q. Salih, A. A. Alsewari, B. Al-Khateeb, M. F. Zolkipli, "Novel Multi-Swarm Approach for Balancing Exploration and Exploitation in Particle Swarm Optimization", The 3rd International Conference of Reliable Information and Communication Technology 2018 (IRICT 2018), Putrajaya, Malaysia, July 2018.

[16] W. Tian and J. Liu, "Network Intrusion Detection Analysis with Neural Network and Particle Swarm Optimization Algorithm", IEEE.978-1-4244-5182-1/10, 2010.

[17] X. Changsheng, "Network Intrusion Detection by using Particle Swarm Optimization and Neural Network", Journal of Networking Technology, Vol. 9, No 1, 2018.

[18] X. Gong and X. Guan, "Intrusion detection model based on the improved neural network and expert system ", DOI: 10.1109/EEESym.2012.6258621, Electrical & Electronics Engineering (EEESYM) Conference, 2012 IEEE Symposium on June 2012.

[19] X. Wang andG. Feng," Research on the Network Intrusion Detection System based on Modified Particle Swarm Optimization Algorithm", 2nd International Conference on Social Science and Technology Education (ICSSTE 2016) DOI: 10.2991/icsste-16.2016.117, January 2016.

[20] X. Yu and C. Estevez, "Adaptive Multiswarm Comprehensive Learning Particle Swarm Optimization". MDPI. Information, Vol.9, Issue 173, doi:10.3390/info9070173, 2018.

[21] Z. Wang, G. L. Durst, E. Lilly, Z. Ben-Miled, "Particle Swarm Optimization and Neural Network", Conference: 18th International Parallel and Distributed Processing Symposium (IPDPS 2004), Santa Fe, New Mexico, USA, March 2004.

[22] B. Durakovic, "Design for Additive Manufacturing: Benefits, Trends and Challenges", Periodicals of Engineering and Natural Sciences Vol.6, No.2, pp. 179-191, ISSN 2303-4521.,2018.

[23] B. Durakovic, "Design of Experiments Application, Concepts, Examples: State of the Art", Periodical of Engineering and Natural Sciences, Vol. 5, No. 3, pp. 421-439, ISSN: 2303-4521., 2018.