A NEW APPROACH FOR WORM DETECTION SYSTEM BASED ON NEURAL NETWORK

Rafik Menassel
Laboratory of Vision and Artificial Intelligence (LAVIA),
Echahid Cheikh Larbi Tebessi University, Tebessa, 12000, Algeria
r.menassel@univ-tebessa.dz

Abdeljalil Gattal
Laboratory of Vision and Artificial Intelligence (LAVIA),
Echahid Cheikh Larbi Tebessi University, Tebessa, 12000, Algeria
abdeljalil.gattal@univ-tebessa.dz

Messai Ahmed
Echahid Cheikh Larbi Tebessi University, Tebessa, 12000, Algeria
ahmedmessai92@gmail.com

Abstract

Among the numerous methods found in the literature that researchers used to develop intrusion detection systems, Artificial Neural Networks (ANN) were the most used machine learning techniques, which is why they were chosen as the main focus in this study, which we relied on to develop a new model that can detect network anomalies. The training stage of ANN is considered the main step of building a predictive model for computer worms to attack, there are different algorithms in the literature to get that done, and including deterministic methods and stochastic ones, each has its pros and cons. to train our proposed model, we relied, within this study, on the improved 'tree-seed algorithm' which is a nature-inspired algorithm. The proposed model was trained with an improved dataset from its predecessor that was extracted from a simulation of the US Air Force network, and it was evaluated based on the test part, which contains types of attacks that the model has not previously trained on, the results obtained indicate good learning capabilities of the proposed model comparing to the results of two other models based on two stochastic algorithms, namely the 'genetic algorithm' and 'particle swarm optimization. The experimental results obtained on, NSL-KDD database show that the proposed scheme achieves interesting performances.

***Keywords*: Intrusion detection system; Worm detection system; Artificial Neural Networks (ANN).**

1. Introduction

Nowadays economy and civilization lean on computer systems and networks which enable a variety of new possibilities such as online conferences, remote works, online social interactions and electronic commerce through its developments. On the other side those systems and networks are ideal targets for computer worms to attack.

One of the frequently asked questions when discussing computer worms is: what are differences between a worm and a virus? [1] although both are considered to be malware, except that they differ on the way they propagate, worms generally have the functionality of self-propagate across networks by exploiting software vulnerabilities and not relying on interactions of users to activate them, viruses rely on user actions to activate and transport them to a new host [1]. However, this difference can blur in case of mass-mailing worms that depend on user to activate them to self-propagate, this study will consider both types as worms and focus on those whom self-propagate across networks.

Maintaining systems and networks security against various types of computer worms can be a challenging task; to increase the security, diverse tools and systems has been developed. Intrusion Detection System (IDS) is a popular one and a widely developed concept in literature. IDS used to monitor behaviors on a single machine or on a segment of a computer network to detect intrusion [2][3][4][5][6], IDS differ in their objectives and implementations techniques, one of the significant capabilities of an IDS, is that it's not only capable of detecting known attacks also new unknown attacks.

Through self-replication and propagation [5] [6], benign worms can fend off harmful worms or fix vulnerabilities in computer nodes. For instance, if host A is aware that host B is susceptible to worm attacks and that host B has a particular vulnerability, host A can automatically transfer harmless worm defense code to host

B using the approved interface to assist host B in repairing the vulnerability or curing the malicious worm infection. As a result, compared to conventional network worms, benign worms are better at spreading themselves independently. Benign worms primarily have the following traits, according to the previous feature description [3] [4]:

- Autonomous defense: non-harmful worms have the ability to defend themselves against viruses and other harmful worms on their own.
- Controllability: Non-host-attacking benign worms can be controlled in their behavior.
- Traceability: The path that benign worms take to spread can be identified.

The network currently contains a variety of resources dispersed throughout. However, a practical approach to integrating these resource data must be proposed. The utilization rate of network resources will increase or network defense capabilities will be strengthened if services are provided by integrating the dispersed computer or data resources in the network. As a result, the purpose of this paper is to improve computer networks by incorporating various types of resource information. The objective of this study also shares some traits with benign worms, which are spread widely and actively have a positive impact on the Internet.

IDS can detect anomalies or unknown attacks by searching for unusual patterns implementing for that prediction techniques such as Artificial Neural Networks (ANN). These are some of the most well-known and strong techniques of machine learning. ANN learns by getting inputs, process them and generate an output, learning can be supervised where the training data have an attached labels as a correct output, unlike unsupervised learning where learning data have no attached outputs on it. [7].

Training ANN can be done with deterministic or stochastic methods, although deterministic methods are simple and fast, they have the problem of initial solution dependency, stochastic methods in the other hand start with random solutions and evolve them to produce better ones, even if they are time consuming, they can get to better results. [7]. Metaheuristic optimizers are a subclass of stochastic methods, with the primary goal of coordinating a learner to find a better solution to a given optimization problem [7]. There are many existing metaheuristic algorithms such as genetic algorithms, particle swarm optimization along others [8].

Tree Seed Algorithms (TSA) is a population-based iterative search algorithm developed By [9], [10] for solving continuous optimization problems, inspired by the relationship of the tree with its seeds, means by which trees spread to the space, those grow over time to become new trees, by considering the spreading space is the search space, the location of trees and seeds are possible solution for the optimization problem, our aim in this study is to train an artificial neural network with improved tree-seed algorithm to develop a new model for anomaly detection.

This paper is structured as follow: After starting by presenting principal keys and concepts of computer worms such as the internal architecture and mechanisms by which it propagates intrusion detection systems. The second section presents some of the related works to give a location of our work, In the third section we dive into artificial networks and how can they be trained, exploring by that metaheuristic optimizers concepts along with a detailed study of the improved tress-seed algorithm, to wrap up with a presentation of NSL-KDD dataset [11], our proposed framework is explained in the fourth section followed by the results and discussions.

2. Related Work

This section focuses on research on training artificial neural networks for anomaly detection with nature-inspired optimizers.

The use of a genetic algorithm to train a feed-forward neural network is covered in [12]. The paper aims to carry out an intrusion detection model by optimizing the weights extraction process, and the trained model achieved a high accuracy rate on testing phase. The work of [13] had developed an approach where a Modified Gravitational Search Algorithm (MGSA) is used to determine the optimum values of weights of a MLP employed to detect anomalous activities in high-speed networks, thus results of testing the trained model in this study showed a higher accuracy and lower alarm rate.

In [14], the authors proposed a method to train a Back Propagation Neural Network (BPNN) model as a network threats detector, based on Artificial Fish Swarming Algorithm (AFSA), they address the problem of falling into local minima, the results in this work showed that the proposed method had higher accuracy and faster convergence speed with the comparison to BPNN, Back Propagation Neural Network by Particle Swarm Optimization (PSO-BPNN), and Back Propagation Neural Network with Genetic Algorithm (GA-BPNN). In [15], an ANN is used to create a learning-based filter to detect spam E-mails, and the authors proposed an optimizing algorithm to set the weights and biases of the Feedforward Neural Network (FFNN) model to the best possible value using a new modified bat algorithm. The show that the concerned model achieved a high generalization performance compared to many other neural networks based meta-heuristics models.

In order to optimize the interconnection weights of the FFNN, develop an artificial neural network with increased precision in classifying malicious from harmless traffic in a network based on Artificial Bee Colony and Particle Swarm Optimization Hybrid Algorithms (ABC-PSO). Results from the trained model compared to

RBF Network, Voted Perceptron, Simple Logistic and Multilayer Perceptron trained models, the comparison reveal that the developed model has higher accuracy and lower error rate. However, the work of [17] developed a learning model for Fast Learning Network (FLN) based on particle swarm optimization (PSO), the model has been applied to classify network activities and detect anomaly, the result of comparing the model against a wide range of meta-heuristic algorithms for training extreme learning machine and FLN classifier disclose that the PSO-FLN has outperformed other learning approaches in detection accuracy.

The authors in [18] propose a new binary classification model for IDS, based on hybridization of Artificial Bee Colony algorithm (ABC) and Dragonfly algorithm (DA) for training an artificial neural network (ANN). The authors extensively compared the results from the trained model against 10 others, the developed model was also assessed against a number of other intrusion detection models designed with a similar principle, the results showed the superiority and the contribution of proposed method on publicly available datasets. Additionally, the study of [19] carried out a new hybrid algorithm between Artificial Bee Colony algorithm (ABC) and Monarch Butterfly optimization (MBO) used to train an ANN such a way that it selects the suitable biases and weights, mainly to detect intrusions in a network, experiment results clearly demonstrated that the proposed approach provided significant improvement compared to nine other optimization algorithms.

The present study is intended to explore the effectiveness of artificial neural networks on the more challenging task of predictive model for computer worm detection. A summary of well-known contributions to historical document writer identification reported in the literature is presented in Table1.

Study			**Database**
Methods	**Classifier**	**metaheuristic algorithm**	
Srinivasu & Avadhani,(2012) [12]	FFNN	GA Weight extraction algorithm	Few rows of 1999 KDD dataset
Sheikhan & Jadidi, (2014) [13]	MLP	MGSA	Flow-based intrusion dataset
Wang, et al. (2015) [14]	BPNN	AFSA	/
Jantan et al. (2017) [15]	FFNN	Modified bat algorithm	SPAMBASE and UK-2011 WEBSPAM datasets
Ghanem, et al. (2018) [16]	MLP	ABC-PSO	KDD Cup 1999 dataset
Ali, et al. (2018) [17]	FLN	PSO	KDD Cup 1999 dataset
Ghanem, et al. (2020) [18]	MLP	ABC-DA	KDD Cup 1999 dataset, NSL-KDD dataset, ISCX 2012 dataset and UNSW-NB15 dataset
Ghanem & Jantan, (2020) [19]	MLP	ABC- MBO	KDD Cup 1999 dataset, ISCX 2012 dataset and UNSW-NB15 dataset

Table 1 Performance comparison of well-known intrusion detection systems

3. Proposed Approach

Metaheuristic based optimization ANNs reside on threes methodologies, at first, the optimization algorithms can be used to find the collection of weights and biases that minimize the error and decrease the cost function for the ANN, secondly, it can be used to find the appropriate structure of the ANN that fit for a particular problem, lastly, it is applicable to adjust a gradient-based learning algorithm parameter. In this work a combination of weights and biases of MLP is optimized using the improved tree seed algorithm in order to develop a network anomaly detector model, to evaluate the developed model GA and PSO algorithms are implemented for the aim of comparing performances. This section aims to presents experiment along with metaheuristic algorithms used for it, to conclude with discussing the obtained results.

3.1. *ANN model*

Although many ANN models have been developed to predict Intrusion detection system over the past several years, additional models are expected to appear in the literature. In this work we are interested in unidirectional data feeding MLP or feed forward neural network (FFNN) with one hidden layer, we donate k the number of input neurons, l the number hidden neurons and m number of output neurons, therefore, the number of weights is calculated as $(k+ m)xl$ and the number of biases is $l+m$ to adopt the collection of weights and biases for the Improved Tree Seed Algorithms (ITSA) [10] an encoding is needed therefore a variable length vector holding floats values is used to represent parameters, Fig 1. illustrate the proposed ANN model.

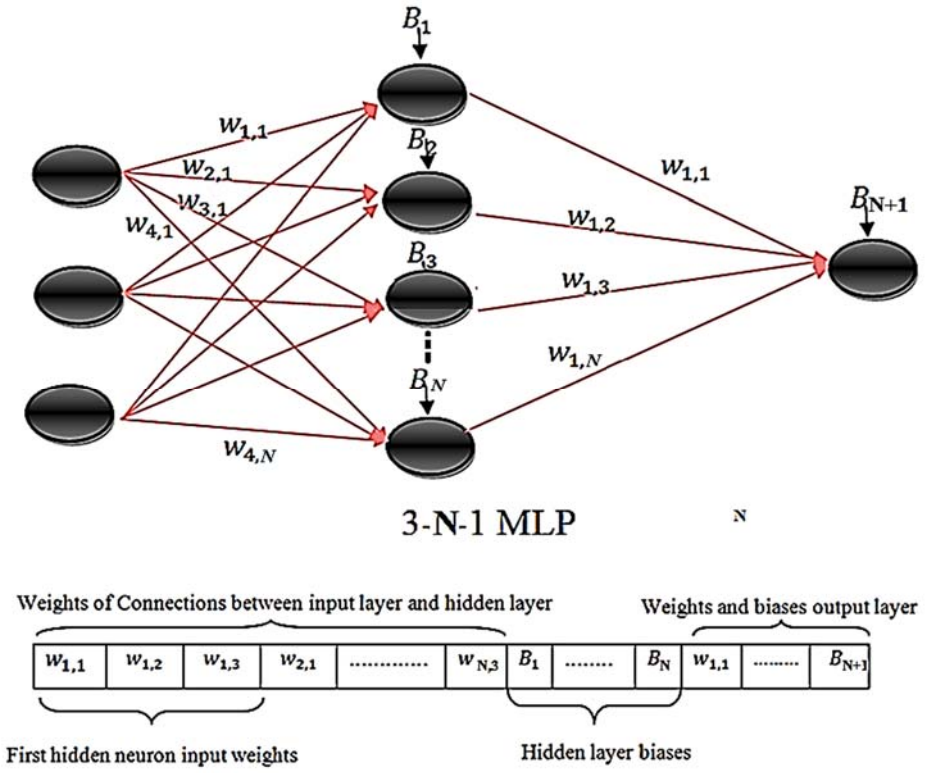

Fig.1. Illustration of our ANN model

Our ANN model includes an input layer, one hidden layer and the output layer.

In this study; we focus on optimizing weights and biases of an MLP with fixed structure, for that a fixed number of neurons is selected previously, input neurons are calculated according to the number of selected features from the NSL-KDD dataset, sixty (60) neurons for the hidden layer, with one output neuron for the reason of classifying feed data as normal or as attack described later in the dataset pre-processing section.

Our ANN model assumes a sigmoid function as a transfer function in both hidden and output layers. However, we tried to set the optimal values of parameters for all three used optimizations algorithms to make their convergence speed to the optimized solution relatively close, therefore, the parameter search tendency (ST) of the ITSA algorithms was set to ST = 0.715 along with boundaries conditions on number of generated seeds for every tree with 10% of the population length as a minimum and 25% as maximum to evade overly long-time execution while training. As recommended in [20], the PSO cognitive and social coefficients (also known as learning factors) were specified with a value of 1.49445 to ensure convergence with ω =0.65 for the weight coefficient. In contrast, GA's four parameters were set to cross rate=0.8, mutation rate=0.08, elite proportion=0.3, and tornement proportion=0.2 as selection parameters. Along with these particular parameters, fifty (50) elements made up each population, which was shared by all algorithms.

3.2. *Improved Tree Seed Algorithm (ITSA)*

The main benefit of meta-heuristics optimization algorithms is the convergence speed to optimum or near-optimum solution for complex optimization problems, TSA as a new nature-inspired algorithms in the literature had difficulties to find the best solution when the dimensions of the problem increase, therefore the authors in [10] proposed some ameliorations to the original TSA to enhance its performance; this section highlight those ameliorations.

To achieve a best exploration and exploitation, acceleration Coefficient C parameter was introduced, which is directly related to the dimensions of the problem and can be calculated according to Eq.1.

$$C = 2 - (D^2 * 0.0001) \quad (1)$$

Every dimension of a generated seeds is affected by a variation factor Δ calculated according to equations (2) and (3) and are also controlled by searching tendency coefficient; as well some restrictions are made on Δ value by setting its lower and higher bounds $\mathcal{M}in$ (Eq.4) and $\mathcal{M}ax$ (Eq.5) respectively to boost the efficiency of the parent tree.

$$\Delta_{i,j} = \left(BestTree_j - Trees_{r,j}\right) * (rand - 0.5) * C \quad (2)$$

$$\Delta_{i,j} = \left(ParentTree_j - Trees_{r,j}\right) * (rand - 0.5) * C \quad (3)$$

$$\mathcal{M}in = -0.1 * (d_{max} - d_{min}) \quad (4)$$

$$\mathcal{M}ax = 0.1 * (d_{max} - d_{min}) \quad (5)$$

d_{max} And d_{min} are outer limits of the search space, as a result the seed dimension now calculated as (6):

$$Seed_{i,j} = ParentTree_j + \Delta_{i,j} \quad (6)$$

3.3. *Fitness function*

There are numerous measures and metrics to evaluate the performance of a neural network model such as Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Normalized Root Mean Square Error (NRMSE), True Positive rate, False Positive rate, F-measure, and accuracy. We choose to use MSE (as shown in Eq.7) as a fitness function due to its widespread use. For that the objective of the ITSA algorithms is to minimize the value of MSE for the neural network model

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (y_i - \hat{y}_i)^2 \quad (7)$$

3.4. *Dataset Preprocessing*

In the first step of NSL-KDD dataset preprocessing, we tried to investigate variation of values among features where we observe that ‘num_outbound_cmds’ and ‘is_host_login’ features were univariate and don’t play a significant role in classification process, for that, we eliminate them. Next, the second step made is to change the ‘label’ column from multiclass to binary class by changing attack labels from its original to be labelled as ‘attack’ as the code shows for both the training set and the testing set.

- Python code to convert the training set's label column from multiclass to binary class.

```
dataframe[’label’]=datafname[‘label’].replace([‘back’,’buffer_overflo
w’,   ’ftp_write’,’guessjasswd’,’imap’,’ipsweep’,’land’,’loadmodule’,
'multihop', 'neptune', 'nmap', 'perl', 'phf', 'pod', 'portsweep',
‘rootkit’,’satan’,’smurf’,’spy’,’teardrop’,’warezclient’,’warezmaster
’],’attack’)
```

- Python code to convert the testing set's label column from multiclass to binary class.

```
dataframe['label']=dataframe['label'].replace([’neptune','guess_passw
d','mscan','warezmaster','apache2','satan','processtable','smurf','ba
ck','snmpguess',’saint','mailbomb','snmpgetattack','portsweep','ipswe
ep’,'httptunnel','nmap','pod','buffer_overflow','multihop','named','p
s','sendmail','rootkit','xterm','teardrop','xlock','land','xsnoop','f
tp_write','perl','phf','worm','udpstorm','sqlattack','loadmodule','im
ap'], 'attack')
```

Because ANN only deals with numerical data, the next step was to encode categorical columns into numerical ones using a 'label encoding' method that involves replacing each value in a column with a number, beginning with 0 and ending with the number of values minus one. The code below selects and encodes all categorical columns at once.

```
cat_colLimns= dataframe.select_dtypes(['category']).columns
dataframe[cat_columns]=dataframe[cat_columns].apply(lambda
x:x.cat.codes)
```

NSL-KDD dataset values are measured on high different scales, feeding a model with such data might end up creating a bias. To address this issue a wise-feature standardization technique is applied on the dataset, the main idea is to standardize columns individually before applying training stage, The standard value of a sample x in column X is calculated as follows:

$$z = \frac{(x - \mu)}{\sigma} \quad (8)$$

where μ is the mean of X, calculated by the equation:

$$\mu = \frac{1}{N} \sum_{i=1}^{N} (x_i) \quad (9)$$

and σ represents standard deviation calculated as:

$$\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^{N} (x_i - \mu)^2} \quad (10)$$

The mean and standard deviation are stored in the first line of the fit transform method to be used on the testing dataset using the transformation method to keep the unseen data. Based on the above, the Fig 2. illustrates our proposed framework for training an MLP with the ITSA algorithm.

The goal of this research is to estimate the weights of an ANN architecture's hidden and output layers using ITSA algorithms during a convergence and accurate estimation process in order to generate accurate results. However, due to the random selection of a sample, the neural network must be left alone in order to provide an accurate answer.

In this study, evaluation metrics such as accuracy (ACC), detection rate (DR), and false alarm rate (FAR) were used for measuring the performance of our proposed model.

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (11)$$

$$DR = \frac{TP}{TP+FN} \quad (12)$$

$$FAR = \frac{FP}{FP+TN} \quad (13)$$

Where:

- True Negative (TN): represents the amount of normal data detected as normal.
- True Positive (TP): represents the amount of abnormal data detected as abnormal.
- False Negative (FN): represents the amount of abnormal data detected as normal.
- False Positive (FP): represents the amount of normal data detected as abnormal.

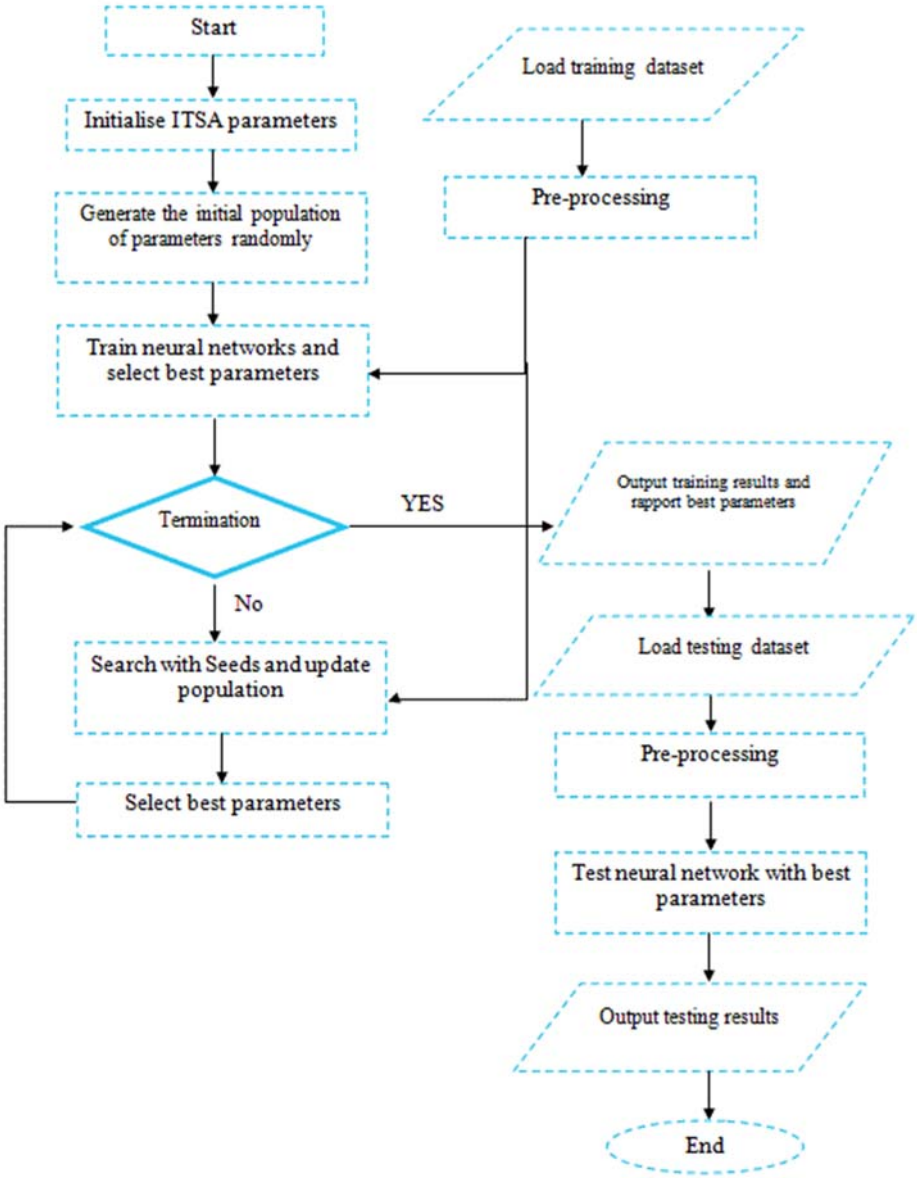

Fig.2. Framework of the proposed approach

4. Results and discussion

The goal of this study is to reduce run-time complexity by 20% from the NSL-KDD train and test dataset by optimizing the set of weights and biases of a Multi-Layer Perceptron (MLP) using the new Improved Tree-Seed Optimization Algorithm (ITSO). The performance of the proposed framework was compared against PSO and genetic algorithms (GA) performances. For each algorithm, we fed to the model for 200 iterations. The outcomes from the training and testing phases are covered in this section.

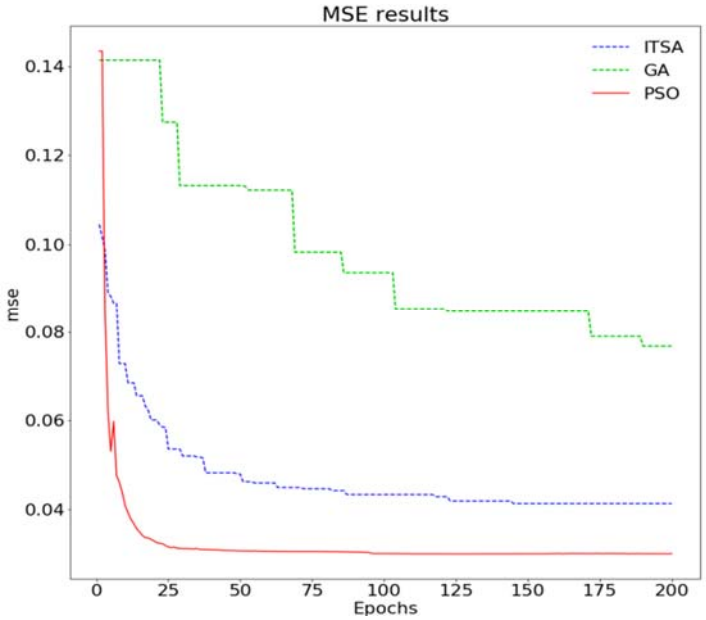

Fig.3. Convergence Curves of three algorithms based on MSE value (MSE Vs epochs)

Figure 3 depicts a representative sample of the convergence plots of all three algorithms toward the best MSE value during training, where ITSA, along with PSO, shows a significant convergence speed, with an approximate average MSE of 0,032 and 0.047 for the PSO and ITSA, respectively, while the rate of convergence in the case of GA was slower. Furthermore, the GA algorithm obtained a lower false alarm rate (FAR) when compared to the other algorithms (average of 200 epochs), despite having a lower accuracy (ACC) and detection rate (DR), as shown in Figure 4, while ITSA and PSO show significantly superior results in those metrics as well as MSE results. Table 2 provides a numerical breakdown of those results.

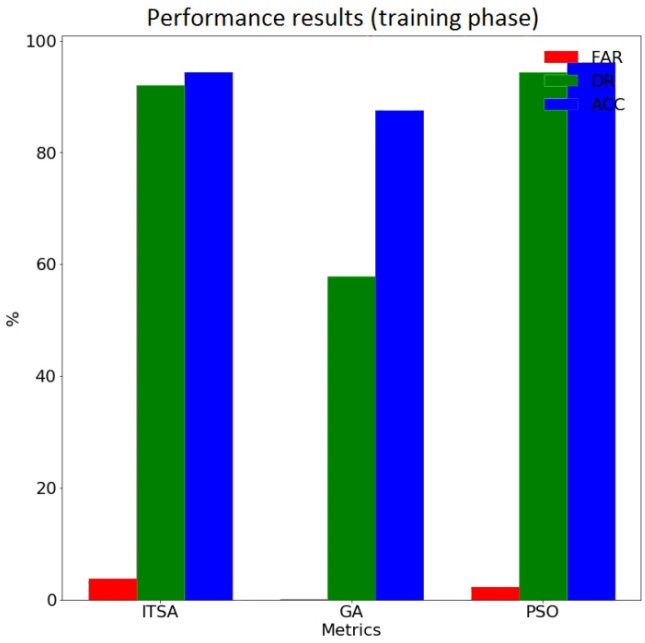

Fig.4 Training performance results

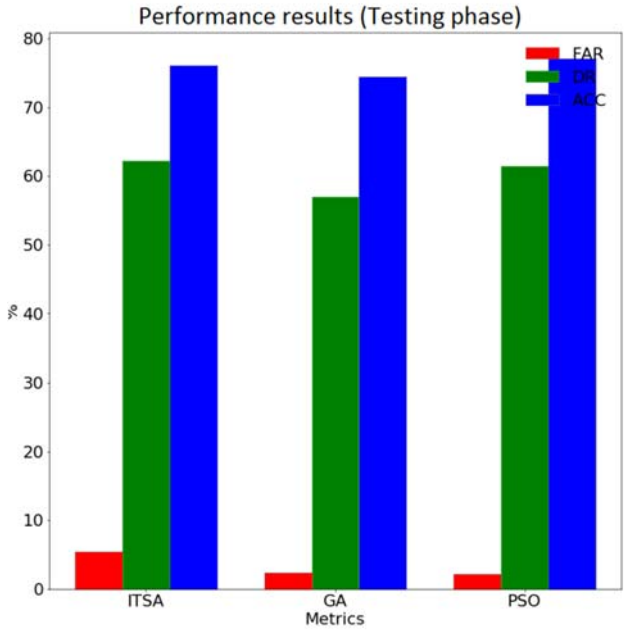

Fig.5. Testing performance results

Figure 5 displays a graphic comparison of the testing performance results obtained by the three algorithms. While we can see the approximate results for the three algorithms when taking into account ACC and DR measurements, ITSA exhibits a higher false alarm rate than the other algorithms. These measurements are also presented numerically in Table 2.

	Training performances				Testing performances			
	MSE	**ACC(%)**	**FAR(%)**	**DR(%)**	**MSE**	**ACC(%)**	**FAR(%)**	**DR(%)**
Proposed Algorithm	0.0474	94.2976	3.7279	91.9963	0.1853	76.0700	5.4723	62.1695
PSO	0.0326	96.1562	2.3322	94.3944	0.2039	77.0680	2.1166	61.3919
GA	0.0989	87.5239	0.0004	57.9664	0.1748	74.4289	2.3748	56.9595

Table 2. Numerical taining/testing preformance results.

In this section, we have introduced the followed methodology to fulfill the development of our proposed model, from parameter representation through data preprocessing toward feeding and testing it with a proportion of the NSL-KDD dataset along with a presentation of approach employed to attain that. The performance of the proposed model shows that a trained Neural Network with the Improved Tree Seed Algorithm can achieve high accuracy and detection rate.

5. Conclusion

Our proposed model is based on training a Multi-Layer Perceptron with one hidden layer using the stochastic algorithm ITSA to detect anomalous behavior, the model has been trained and evaluated with the NSL-KKD dataset and its performance compared against the performance of two most widely known metaheuristic algorithms namely Genetic Algorithms (GA) and Particle Swarm Optimization (PSO), satisfying results has been obtained considering the few numbers of feed data.

Despite the invested time and effort to develop new detection and counter-measure approaches, it cannot be said that the situation is stable; as a matter of fact, more sophisticated and more complex generation of worms is already spreading, especially with the development of smart phones that maybe will the next target for new worm major attack.

Conflicts of Interest

The authors have no conflicts of interest to declare.

References

[1] Smith, C., Matrawy, A., Chow, S., & Abdelaziz, B. (2009). Computer worms: Architectures, evasion strategies, and detection mechanisms. Journal of Information Assurance and Security, 4, 69-83.
[2] Srinivasu, P., Avadhani, P. S. (2012). Genetic algorithm based weight extraction algorithm for artificial neural network classifier in intrusion detection. Procedia engineering, 38, 144-153.
[3] Shi, L., Li, X., Gao, Z., Duan, P., Liu, N., & Chen, H. (2021). Worm computing: A blockchain-based resource sharing and cybersecurity framework. Journal of Network and Computer Applications, 185, 103081.
[4] Chen, Y., Yang, X., Li, T., Ren, Y., & Long, Y. (2022). A blockchain-empowered authentication scheme for worm detection in wireless sensor network. Digital Communications and Networks.
[5] Mallik, A., Khetarpal, A. & Kumar, S. ConRec: malware classification using convolutional recurrence. J Comput Virol Hack Tech 18, 297–313 (2022). https://doi.org/10.1007/s11416-022-00416-3
[6] Zhou, H., Hu, Y., Yang, X., Pan, H., Guo,W. , Zou, C. C. "A Worm Detection System Based on Deep Learning," in IEEE Access, vol. 8, pp. 205444-205454, 2020, doi: 10.1109/ACCESS.2020.3023434.
[7] Cinar, A.C. Training Feed-Forward Multi-Layer Perceptron Artificial Neural Networks with a Tree-Seed Algorithm. Arab J Sci Eng 45, 10915–10938 (2020). https://doi.org/10.1007/s13369-020-04872-1
[8] Martins, S.L., Ribeiro, C.C. (2006). Metaheuristics and Applications to Optimization Problems in Telecommunications. In: Resende, M.G.C., Pardalos, P.M. (eds) Handbook of Optimization in Telecommunications. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-30165-5_4
[9] Mustafa Servet Kiran, TSA: Tree-seed algorithm for continuous optimization, Expert Systems with Applications, Vol. 42, Issue 19, 2015, Pages 6686-6698, https://doi.org/10.1016/j.eswa.2015.04.055.
[10] Aslan, M., Beşkirli, M., Kodaz, H., & Kiran, M.S. (2018). An Improved Tree Seed Algorithm for Optimization Problems. International Journal of Machine Learning and Computing, vol. 8, no. 1, pp. 20-25, 2018.
[11] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), 2009.
[12] P. Srinivasu, P.S. Avadhani, Genetic Algorithm based Weight Extraction Algorithm for Artificial Neural Network Classifier in Intrusion Detection, Procedia Engineering, Volume 38, 2012, Pages 144-153, https://doi.org/10.1016/j.proeng.2012.06.021.
[13] Sheikhan, M., Jadidi, Z. Flow-based anomaly detection in high-speed links using modified GSA-optimized neural network. Neural Comput & Applic 24, 599–611 (2014). https://doi.org/10.1007/s00521-012-1263-0
[14] Wang, T., Wei, L., & Ai, J. (2015). Improved BP Neural Network for Intrusion Detection Based on AFSA. Proceedings of the 2015 International Symposium on Computers & Informatics. Atlantis Press, Pages 373-380.
[15] Jantan, A.B., Ghanem, W.A., & Ghaleb, S.A. (2017). USING MODIFIED BAT ALGORITHM TO TRAIN NEURAL NETWORKS FOR SPAM DETECTION. Journal of Theoretical and Applied Information Technology: Vol. 95. No.24 - pp. 6788-6799.
[16] Ghanem, W.A., & Jantan, A.B. (2018). New approach to improve anomaly detection using a neural network optimized by hybrid ABC and PSO algorithms. Pakistan Journal of Statistics. 2018. - Vol. 34. pp. 1-14.
[17] Ali, M. H. Al Mohammed, B. A. D., Ismail, A. , Zolkipli, M. F., "A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization," in IEEE Access, vol. 6, pp. 20255-20261, 2018, doi: 10.1109/ACCESS.2018.2820092.
[18] Ghanem, W.A.H.M., Jantan, A., Ghaleb, S. A. A. , Nasser, A. B., "An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons," in IEEE Access, vol. 8, pp. 130452-130475, 2020, doi: 10.1109/ACCESS.2020.3009533.
[19] Ghanem, W.A.H.M., Jantan, A. Training a Neural Network for Cyberattack Classification Applications Using Hybridization of an Artificial Bee Colony and Monarch Butterfly Optimization. Neural Process Lett 51, 905–946 (2020). https://doi.org/10.1007/s11063-019-10120-x
[20] Clerc, M, Kennedy, J., "The particle swarm - explosion, stability, and convergence in a multidimensional complex space," in IEEE Transactions on Evolutionary Computation, vol. 6, no. 1, pp. 58-73, Feb. 2002, doi: 10.1109/4235.985692.

Authors Profile

RAFIK MENASSEL was born in Algeria. He received his BS degree in Computer Science from University of Mentouri-Constantine (Algeria) in 2006, MS degree in Computer Science "Information and knowledge systems" from Echahid Cheikh Larbi Tebessi University, Tebessa (Algeria) in 2009 and he received a PhD in computer science from Badji Mokhtar- University, Annaba, Algeria in 2018. Following his PhD, he worked as an Associate professor in the department of Mathematics and Computer Science, University of Tebessa, Tebessa, Algeria, where he did research in the areas of biometrics, writer identification, image processing, image compression and document analysis. He has published various papers in the above general areas.

ABDELJALIL GATTAL was born in Algeria. He received his BS degree in Computer Science from University of Skikda (Algeria) in 2004, MS degree in Computer Science "Information and knowledge systems" from Abbes Laghrour University of Khenchela (Algeria) in 2009 and He received his PhD in 2016 from Ecole nationale Supérieure d'Informatique (ESI-Algeria) in Computer Science and focuses in Segmentation-Verification for Handwritten Digit Recognition. Currently, he is working as Full Professor at the Department of Mathematics and Computer Science in University of Tebessa (Algeria). He supervised many Master and License students. He has published a number of papers. In addition, He has collaborated as a member on several research projects and also participated in several scientific competitions. His research interests include Image Analysis, Pattern Recognition and Recognition of handwriting

AHMED MESSAI was born in Algeria in 1992, he received his Master degree in Computer Science " networks and IT security" from Echahid Cheikh Larbi Tebessi University, Tebessa (Algeria) in 2021.