Wasit Journal for Pure Science

Journal Homepage: https://wjps.uowasit.edu.iq/index.php/wjps/index
e-ISSN: 2790-5241 p-ISSN: 2790-5233

Network intrusion detection using optimal perceptron with cuckoo algorithm

Hameed Lafta Saad[1]

[1]Islamic Azad University Science and Research Brach, Computer engineering field, Computer Network, IRAN

*Corresponding Author: Hameed Lafta Saad

DOI: https://doi.org/ 10.31185/wjps.326
Received 02 January 2024; Accepted 17 March 2024; Available online 30 March 2024

ABSTRACT:
To safeguard computer networks from intruders, intrusion detection systems have been created. These systems operate in conjunction with firewalls and other security measures to guarantee the safety and efficiency of the computer system. An intrusion detection system is a tool designed to detect and pinpoint attacks and vulnerabilities within a network or computer system. It subsequently notifies the system administrator of them. The primary challenge with intrusion detection systems is enhancing their speed and precision in detecting intruders. This article explores a novel technique for identifying attempts to infiltrate computer systems. The system utilizes a hybrid approach involving the cuckoo algorithm and perceptron neural network. This novel approach can detect intrusion data more accurately than previous methods and enhance the detection rate by over 1%. The system utilizes the cuckoo method to choose a subset of characteristics, which are then analyzed based on the frequency of various attribute types in intrusive and normal data using an optimum perceptron. The system has been evaluated and the implementation has yielded a detection accuracy of 89.8%, representing a substantial enhancement compared to earlier approaches.

Keywords: intrusion detection systems, data mining attack, cuckoo algorithm, perceptron,

1. INTRODUCTION

Today, the conversation surrounding system security and intrusion detection plays a crucial role in addressing computer and network security concerns. It has fulfilled security objectives. Securing computer systems and networks has become increasingly crucial due to the rising use of computer networks, particularly the Internet, the advancing expertise of users and attackers, and the presence of multiple software vulnerabilities. Research and inquiry on non-preventive systems like intrusion detection systems, which identify attacks and aberrant behaviors in computer systems and networks, are also crucial and hold a distinct standing. Intrusion detection systems monitor computer systems or networks to analyze events and detect deviations from security policies [1-2].

An extremely basic definition of an intrusion detection system is a computer and network danger notification system. In order to improve their intrusion detection capacity, modern intrusion detection systems leverage more comprehensive information sources than their predecessors. These information sources include a number of extraneous details that the detection engine may choose to ignore. They vary depending on the intrusion detection system's architecture and the locations of the sensors that are in charge of gathering primary data. There are two methods that intrusion detection systems can employ to spot questionable activity. In order to determine whether or whether the conduct under investigation deviates from what is considered "norm behavior," profiles of users' typical behavior are created and compared with other actions. This process is known as intrusion diagnosis and intrusion detection. Subsequently, the intrusion detection system searches for actions that have been previously classified as attacks. Having at least one history of experiencing such conduct in the past is necessary to determine whether a behavior is included in known attacks or not. There are restrictions on single-neuron networks, such as their inability to perform non-linear functions [3].

Using a new network architecture and an advanced learning algorithm, Chiba et al. [4] have given the best way to construct an intrusion detection system in a posterior neural network network. For the first time, this method depends on creating every possible combination of the right values for the parameters that can be used to build such a classification, or on how well the parameters—such as selection, data normalization feature, neural network architecture, and activation function—perform in terms of anomaly detection. Lazy learning techniques have been suggested by Chelam et al. [5] as a way to enhance intrusion detection systems' general performance.

In order to attain greater accuracy and quicker detection times, Wang et al. [6] have introduced a network intrusion detection system that uses a machine learning algorithm to detect or block network intrusions. Another significant benefit is the application of machine learning, which reduces the need for advanced knowledge compared to the black and white list model. With the use of a supervised learning algorithm, Ashfaq et al. [7] introduced a fuzzy-based semi-supervised learning technique that uses unlabeled data to enhance intrusion detection system classification performance. To guarantee that pertinent and implicit information will be retrieved from the data that is of interest to the user and has a shorter execution time, Vishwakrama et al. [8] have combined the idea of data mining with intrusion detection systems.

A novel multi-stage decision tree algorithm and support vector machine were introduced by Amno et al. [9] to enhance threat classification and, consequently, security solutions. An effective fuzzy clustering technique for network intrusion detection was developed by Li et al. [10]. An algorithm based on clustering has been used in a cloud storage environment to detect intrusions from mobile ad hoc networks.

A system that applies a number of pre-processing procedures to the sensor results is reported in the study by Waller et al. [11].

In order to detect misuse and anomalies, Hrong et al. [12] proposed a hybrid intrusion detection system that included protocol analysis with data mining techniques. Experiment results show that our proposed method can achieve a good and robust performance, which possesses huge competitive advantages when compared to other existing methods in terms of accuracy, detection rate, false alarm rate and training speed. A new approach based on the coupling of the hierarchical clustering algorithm and the straightforward feature selection process of support vector machine techniques was introduced by Chisler et al. [13]. Hierarchical clustering gives the support vector machine model greater quality training data. This approach shortens the training period while also increasing productivity. A technique based on threat notification correlation was presented by Gang et al. [14]. In order to combat computer assaults, this strategy aims to densify the notice of threats and their linkage. This article introduces a novel concept on the integration of two detection systems. To improve the caliber of information gleaned from them, different influences are dependent on behavior and expertise.

In the study conducted by Lee et al. [15], they proposed a method based on genetic network programming and association rules to identify network penetration by combining anomaly and utilization. Make distinctions between unknowns. A strategy based on feature reduction and support vector machines was presented by Zhou et al. [16]. This approach used the support vector machines and ant community algorithm clustering techniques to give a high intrusion detection rate.

. A novel strategy was put up in [17] To find a good balance between trying new things and using what already works, and also fix the problem of getting stuck on something that's not the best. This was done by making the MFO (Moth–Flame Optimization) better and adding new operators along with the embedded spiral operator. This work's main idea is using the cosine similarity measure to change the continuous MFO into a binary problem. The limits of the commonly used sigmoid function, which relies on a threshold value for conversion, are solved by using cosine similarity. However, cosine similarity measures how much alike the current and ideal solutions are. The authors of [18] suggested hybridizing modified binary GWO with PSO. The suggested solution outperformed the previous solutions, as evidenced by the two benchmarking datasets it employed, NSL KDD'99 and UNSW-NB15. The suggested approach increased detection accuracy by roughly 0.3% to 12% and detection rate by 2% to 12%. Furthermore, false alarm rates are decreased by 4% to 43%, and between 31% and 75% less characteristics are present. In conclusion, the suggested method lowered processing time by roughly 14% to 22% in comparison to cutting-edge methods.

In [19], Multilayer Perceptron learning is optimized by the use of the Harris Hawks Optimization algorithm (HHO) in an Intrusion Detection System (IDS) to adjust weight and bias settings. The goal of this method learning process is to choose the best parameters in order to reduce network intrusion detection errors.

The low accuracy of common intrusion detection system methods is a problem that this research aims to address with a novel method. An intrusion detection system is a piece of hardware or software that watches the sequence of events to identify threats. In order to completely secure a computer system, intrusion detection systems are required in addition to firewalls and other intrusion prevention tools. This way, in the event that an intruder manages to get past the firewall, antivirus software, and other security tools and into the system, the system can identify the threat and devise a countermeasure. The Cuckoo algorithm is the one employed in this study. Among the most advanced and potent evolutionary optimization techniques ever presented is this algorithm.

2 THE PROPOSED DETECTION METHODOLOGY

The proposed method involves generating a set of reduced characteristics using the cuckoo search algorithm and designing an intrusion detection system using a perceptron neural network.

2.1 Perceptron network

Engineers utilize artificial neural networks as significant tools. The perceptron neural network, also known as the perceptron learning rule, is the simplest form of artificial neural network. Understanding the perceptron method is crucial as it forms the foundation for comprehending artificial neural networks. Artificial neural networks are computational algorithms designed to mimic the functioning of the human brain. They have gained popularity in recent times. People are attentive to them due to their proficiency in problem-solving and their applicability across several fields of study. They can be utilized for supervised learning to solve problems with known answers or for unsupervised learning when the answer is unknown.

This section requires a discussion of the architecture of the perceptron network. Figure 1 displays the Perceptron neural network.

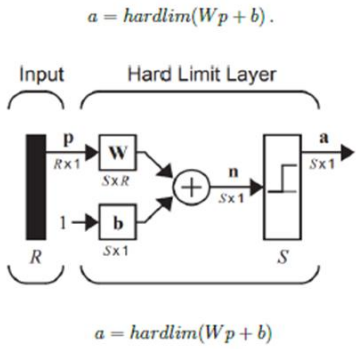

Figure 1. perceptron network [20]

First, the weight matrix of the network is considered:

$$W = \begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,R} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,R} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ w_{S,1} & w_{S,2} & \cdots & w_{S,R} \end{bmatrix} \quad 1.$$

W will be as follows:

$$W = \begin{bmatrix} {}_1W^T \\ {}_2W^T \\ \vdots \\ {}_3W^T \end{bmatrix} \quad 2.$$

Therefore, the i-th element of the output vector will be the following Eq.

$$a_i = hardlim(n) \quad 3.$$
$$= hardlim({}_iw^T p + b_i):$$

where the hardlim transfer function is defined as follows:

$$a_i = hardlim(n) \quad 4.$$
$$= \begin{cases} 1 & if \geq 0 \\ 0 & otherwise \end{cases}$$

2.2 Cuckoo algorithm

One technique for handling complex, never-ending problems is the Cuckoo Algorithm. The lifestyle of a species of birds known as "cuckoos" has an impact on this computer program. We use the behavior of a Cuckoo bird as inspiration while writing computer programs. This bird is distinct in that it can estimate and reproduce. The Cuckoo Optimization Algorithm is initiated using Cuckoo eggs and adult male birds that are sterile. Adult Cuckoos lay their eggs in several birdhouses. The cuckoo eggs will hatch into adult cuckoo birds if the birds do not find and kill them. Because their choices can be influenced by their surroundings, adult cuckoos migrate in groups to choose an appropriate location for

living and reproducing. The "global optimum" is the best solution that this computer software seeks to identify. This approach has been shown to be effective in a variety of real-world scenarios. The cuckoo bird algorithm was introduced by Ying and colleagues in 2008 [21]. Because of their peculiar lifestyle and tendency to raise their generation as parasites, cuckoo bird species served as an inspiration for this algorithm.
This stage determines the parameters of the algorithm. These parameters are: the algorithm's population, or the number of nests, (n); the algorithm's step size parameter, (a); the algorithm's detection probability, (Pa); and the maximum number of penetration analyses required to halt the method.

2.2.1 Primary population production

The initial location of the nests at this stage is randomly determined from among the sections considered for each design variable in the following form:

$$nest_{i,j}^{(0)} = (X_{j,\min} + rand.(X_{j,\max} - X_{j,\min}) \quad 5.$$

so that $nest_{i,j}^{(0)}$ is the initial location of the jth variable from the ith nest or solution, $X_{j,\max}$ and $X_{j,\min}$ are the minimum and maximum values For the variable or group of jam and rand, it is a random number from the interval [0,1].

2.2.2 Birth of new cuckoos using Levy's flight pattern

At this stage, all the nests, other than the best nest or solution obtained so far, are replaced by using newly created eggs from the location of the nests according to the quality of the solution in the following form:

$$nest_i^{(t+1)} = nest_i^{(t)} + \alpha.S.(nest_i^{(t)} - nest_{Best}^{(t)}) \quad 6.$$

so that $nest_i^{(t)}$ is the current location of the i-th nest. α is the probability parameter, S is the Levi's flight vector based on Mantagta's algorithm, which is presented in equation 7. r is a random number from the standard normal distribution and $nest_{Best}^{(t)}$ is the best nest or solution obtained so far.

$$s = rand.(nests[permute\ 1[i][j] - nests\ [permute\ 2[i][j]) \quad 7.$$

Where Pamute 1 and Permute 2 are permutation functions that are applied on the rows of the matrix related to the solutions and P is the probability matrix introduced in the following relationship.

$$p_{i,j}\begin{cases} 1 & if\ rand < pa \\ 0 & if\ rand \geq pa \end{cases} \quad 8.$$

2.2.3 Discover strange eggs

Strange eggs are discovered using the probability matrix explained in equation 9 for all variables of all nests. Existing nests are based on quality, solving with newly created eggs through random moves with random steps. They are replaced by the following form.

$$nest^{(t+1)} = nest^{(t)} + s.* p \quad 9.$$

The host bird will either discard the cuckoo egg or leave the nest if it discovers one in its nest. The fundamental ideas behind the cuckoo search algorithm are these two phenomena. This algorithm's primary characteristics are:
A cuckoo deposits an egg in a nest that it chooses at random. It stands for a potential fix for an optimization issue. The best solutions are retained, and the nest containing the best egg is advanced to the following iteration.
To eliminate noise and unnecessary information, each cuckoo egg deposit has a chance of Pa € {0, 1}. The total number of possible nests is set. Among the most important techniques utilized in data preprocessing are data cleansing, transformation, integration, and reduction. To balance the data in accordance with the suggested manner, the pre-processing procedures of data transformation and data normalization have been completed in the current work. Until the algorithm hits a stopping threshold, the two steps pertaining to the creation of fresh cuckoo eggs and the discovery of stranger eggs are alternately repeated. This algorithm's maximum number of analyses can be thought of as a terminating condition [22].

This section discusses the creation of an intrusion detection system that uses a perceptron neural network and the Cuckoo algorithm. Given that choosing features is an essential first stage in the design of an intrusion detection system. First, the concepts needed for the construction of the new technique are given, and then the system is built. The Cuckoo algorithm was used to pick the feature, and the optimal perceptron neural network was used to design the intrusion detection system.

One of the fundamental processes in intrusion detection systems is feature selection, as was covered in the prior content. The set of reduced features in this study is chosen using the cuckoo algorithm approach. The number of each sample of data in each of these attributes is determined after the set of reduced attributes is created, and based on the data set, a perceptron neural network is used to detect the effect or normality of the data. The system will then be tested using the data set to ascertain whether or not the data is intrusive.

Levy fly is used by the Cuckoo search method in place of random walk, which enhances performance. Typical Levy flight features have been seen in a wide variety of animals and insects. A Levy flight is a random walk with a heavy-tailed probability distribution controlling the step length. After taking a lot of steps, a random walk's distance from its beginning tends to a stable distribution. Gandami and his colleagues [23] make this clear. Levy flying does a better job of performing that random walk. As a result, the cuckoo search algorithm was used for this study since it offers a quicker rate of convergence.

In the suggested strategy, where initial weights and matching biases are chosen for perceptron optimization, each optimal nest indicates a potential solution. The optimization of weight and population size determines the quality of the solution. The method operates in two stages. The best weight and bias for the first cycle are initialized using the Cuckoo method in the first step. Second, the weights are compared to the optimal solution by the use of backpropagation. The Cuckoo algorithm repeats this procedure, updating the weights with the best available answer each time and looking for the ideal weights until the very end of the cycle.

The suggested method's flow is depicted in Figure 2, wherein (i) a population of n nests is randomly started to create the optimal perceptron, and (ii) a new solution (nest) is obtained through Levy flight and its fitness is assessed.

(iii) The optimal solution is determined by comparing the new and old solutions after each cycle.

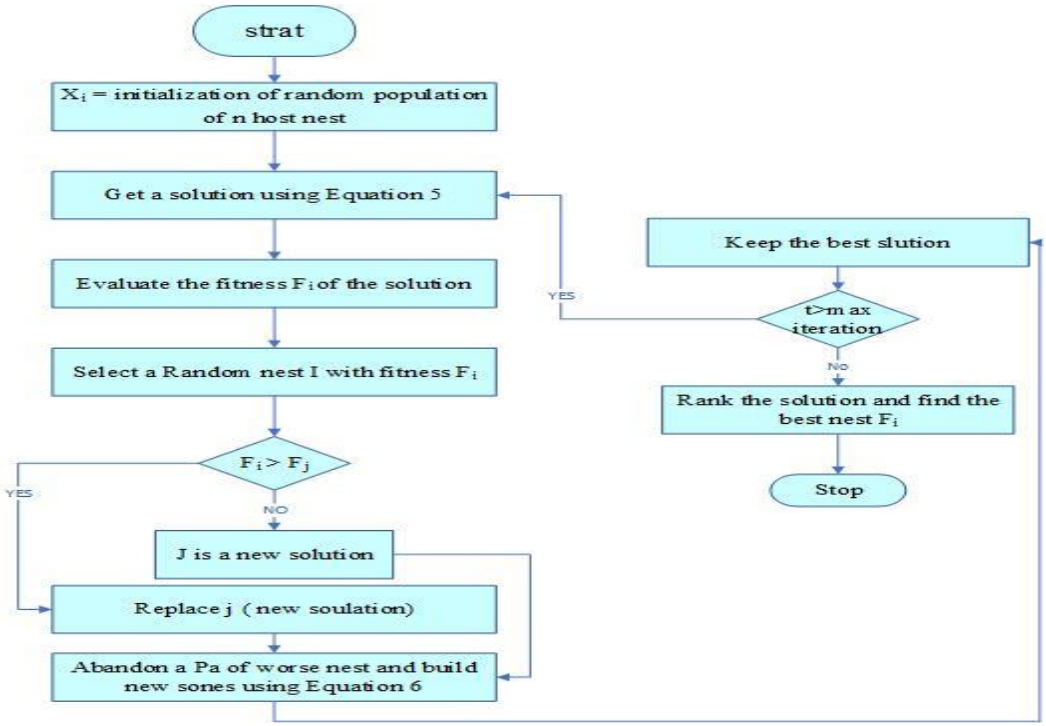

Figure 2. Flow of the proposed method

According to the proposed method, X_i = initialization of a random population of n host nests. In the next step, a solution is obtained using equation 15-3. The suitability Fi of the solution is evaluated and according to the equation 3-16, a random nest (i) is selected with the suitability (F_i). If $F_i > F_j$, j is a new solution, and if it is, j is replaced (new solution). A P_a is discarded from the worse nest and new nests are constructed using Equation 6, and this process is repeated until the solutions are ranked and the best Nest F_i is found.

2.3. **Comparison criteria**

Two key aspects related to the evaluation and as a result comparing the performance of intrusion detection approaches are: the efficiency of the detection process and the operation cost. In addition to not underestimating the importance, the cost should be emphasized. In this context, there are four modes corresponding to the relationship between the detection results for an analyzed event ("normal" vs. "intrusion") and the true nature of the results ("harmless" vs. "malicious").
These four modes are:
True Positive (TP): The analyzed event is correctly detected as an intrusion.
False Positive (FP): The analyzed event is harmless from a security point of view, but is detected as malicious.
The true negative (TN) of the analyzed event is correctly recognized as safe and normal.
False negative (FN): The analyzed event is malicious but is recognized as harmless.
It is clear that the lower the FP and FN and the higher the TP and TN, the better the performance.
The main purpose of this paper is to provide a method to improve the intrusion detection system in computer networks using neural networks and cuckoo algorithm. In this paper, the system evaluation system has been done based on the relevant criteria in the field of intrusion detection, which include accuracy, precision, intrusion detection rate, error warning rate, readout (False Positive Rate), sensitivity rate, F-measure, and the results The result is compared with FC-ANN and genetic algorithm methods.

2.3.1 **Simulation scenario**

Pre-processing processes are carried out in accordance with the KDD98 database, which is the first consideration in simulating the suggested method. Following the data pre-processing procedures, a few of the most significant and crucial data features—known as heading features—are taken out and sent into the neural network as input. because there are three levels in a neural network: input, hidden, and output

2.3.2 **Data model**

The IST group from MIT Lincoln Laboratory under DARPA collected the first standardized data for the review and evaluation of intrusion detection systems. This information was used over several weeks in a simulation to test DARPA's [1]intrusion detection system. This data set is classified based on the year of data collection (1998-1999). The data set of 1999, which was collected with his diligence and under his supervision and during his PhD project, was used in the third international competition of knowledge discovery and data mining KDD-CUP99 and in the fifth conference in this field. Contains standard connection records that include a set of simulated attacks and intrusions on a military network.

3. **RESULT**

MAE is the sum of positive errors for all values. It is calculated by finding the difference between the actual value and the predicted value and taking their absolute value. The positive value of all errors is taken and the average is calculated using Equation 10.

$$MAE = \frac{\sum_{i=1}^{n} |y_i - x_i|}{n} \qquad 10.$$

Where y_i is the actual value, x_i is the predicted value, and n represents the total number of data points in the dataset. Figure 3 shows the MAE result and its convergence during the experiments for the proposed method for the test and training data sets. MAE starts at 1.2323 and continuously decreases to 0.011163 after 500 periods. As shown in the MAE plot for the test data set. After 500 to 1000 cycles, the change in MAE value is negligible as shown by a straight line in the graph. The final calculated value for MAE in our experiment is 0.0097501. Similarly, the calculated MAE value on the test data set starts at 0.07123 and then continuously decreases to 0.001244 after 120 epochs. The MAE value remains almost constant up to 1000 periods.

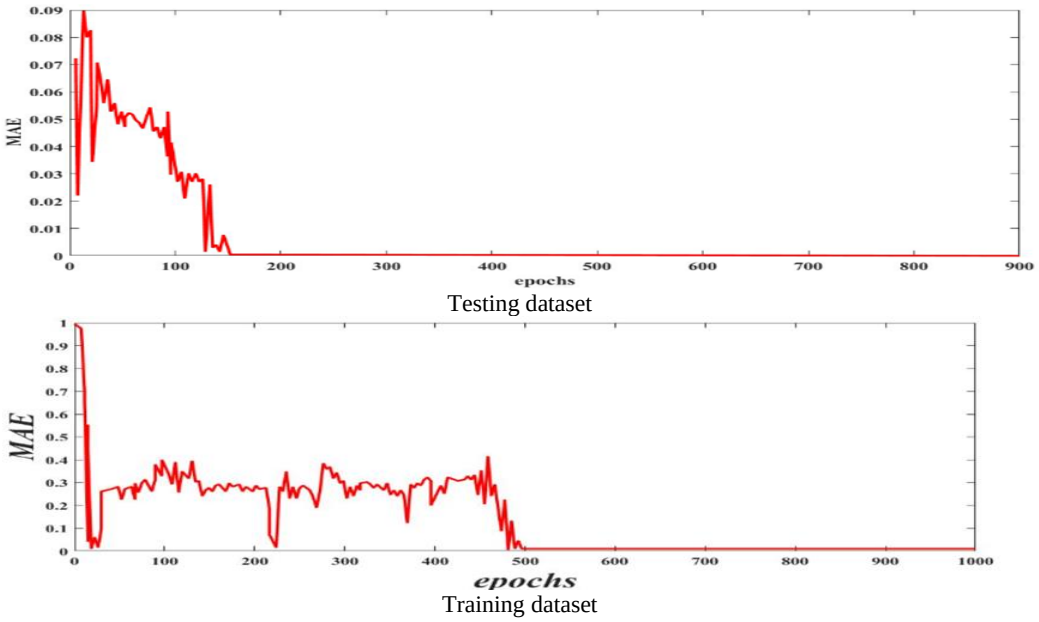

Figure 3. MAE convergence for testing and training datasets

In this research, the values of the proposed method are compared with the following three methods.
• Method based on ad hoc wireless networks (CWN) [23]
• Method based on service quality and parallel technology (SQPT) [24]
• Combined genetic and fuzzy method (GF) [25]
Table 1-4 shows the MEA values for these three methods and the proposed method. As can be seen, the sum of positive errors for the proposed method is the smallest. As shown in Table 1, the proposed model outperforms other models in terms of MAE.

Table 1. MAE values for conventional methods

	proposed method	CWN	SQPT	GF
MAE	**0.0097501**	**0.0097100**	**0.0096021**	**0.0096541**

a. Accuracy

In the evaluation of intrusion detection, we know that in order to obtain the accuracy of intrusion detection, the ratio of the sum of true positives and true negatives to the sum of true positives, false positives, true negatives, and false negatives is shown in relation 11 to show the accuracy of the proposed method with other methods. Shows in Figure 4. The accuracy for the proposed method is 0.898, which is higher than other common methods.

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \quad 11.$$

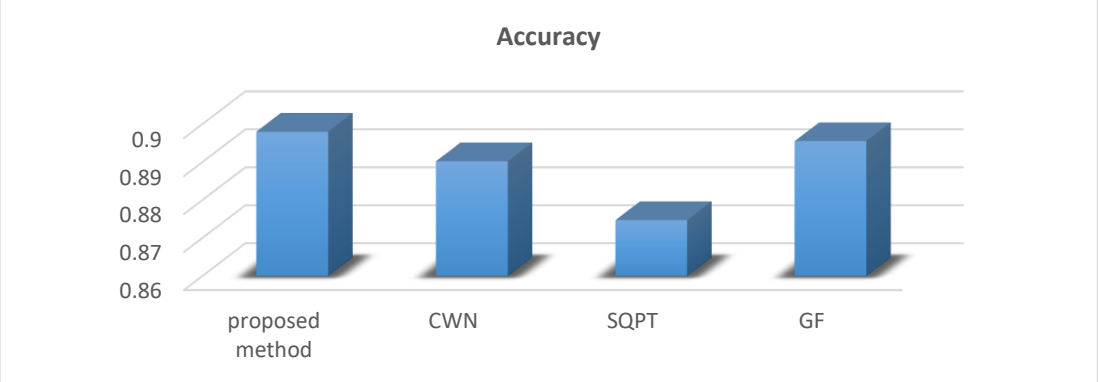

Figure 4. Comparison of the accuracy of the proposed method and conventional methods

b. Precicion

In terms of evaluation, the higher the Precicion, the more secure the system is. Which is the ratio of true positives to the sum of true positives and false positives in order to obtain and calculate the accuracy of intrusion detection. Which shows the accuracy of the proposed method with other methods in relation 12 in Figure 5. The Precicion for the proposed

method is 0.9341, which is higher than other common methods and the system has more security.

$$\text{Precicion} = \frac{TP}{TP + FP} \qquad 12.$$

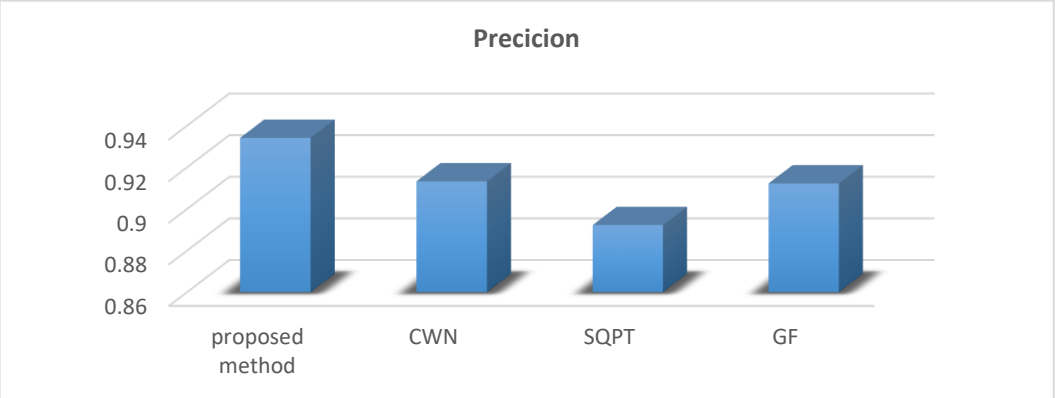

Figure 5. Comparing the Precicion of the proposed method and conventional methods

c. False Positive Rate

In the False Positive Rate or the FPR, the closer the value is to zero, the system has the minimum error, and in order to obtain and calculate the error alarm rate in intrusion detection, the obtained accuracy value is subtracted from one (1). In the equation 13 shows the error warning rate with the proposed method compared to other methods in Figure 6. The False Positive Rate for the proposed method is 0.0659, which has less error than other common methods.

$$\text{FPR} = 1 - \frac{TP}{TP + FP} \qquad 13.$$

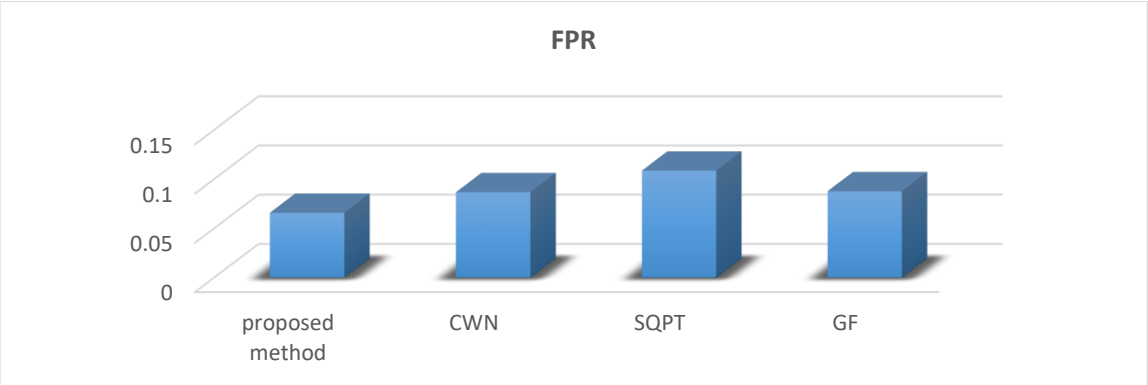

Figure 6. Comparison of the False Positive Rate of the proposed method and conventional methods

d. Recall

Recall is usually called True Posetire Rate, the closer it is to one, the more efficient the system is. Equation 14 shows the display and loading of the proposed method with other methods in Figure 7. The error warning rate for the proposed method is 0.9913, which is higher than other common methods and is a sign of the efficiency of the method.

$$\text{Recall(TPR)} = \frac{TP}{TP + FN} \qquad 14.$$

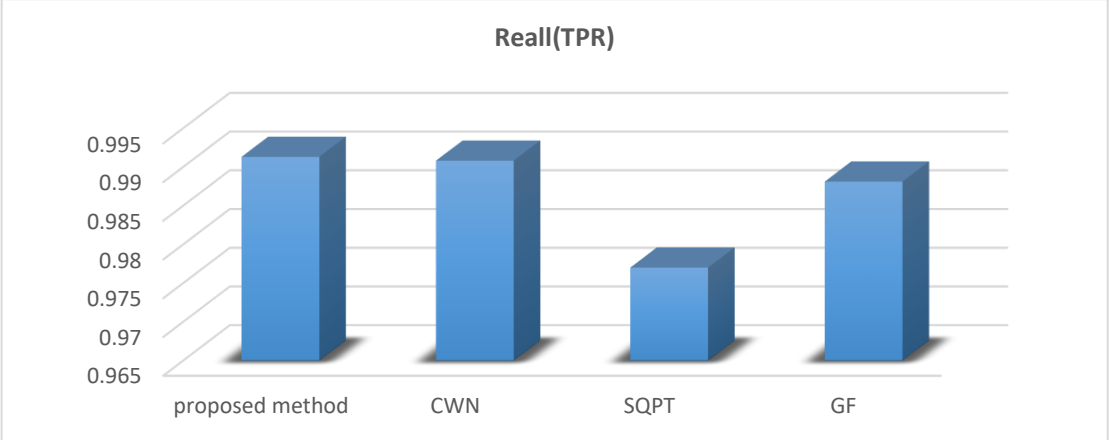

Figure 7. Comparing the Recall of the proposed method and conventional methods

e. F-measure

F-measure, which is a combination of accuracy and readability criteria presented by van Rijsbergen in 1974 [26], is one of the usual evaluation criteria, especially when working with unbalanced sets. Which shows the proposed method with other methods in Figure 8 in the equation 15 representations F-measure. F-measure, which is a combination of accuracy and readability criteria, is 0.977 for the proposed method, which is higher than other common methods and is a sign of the efficiency and accuracy of the method.

$$\mathrm{F-measure} = \frac{2 * Precision * Recall}{Precision + Recall} \qquad 15.$$

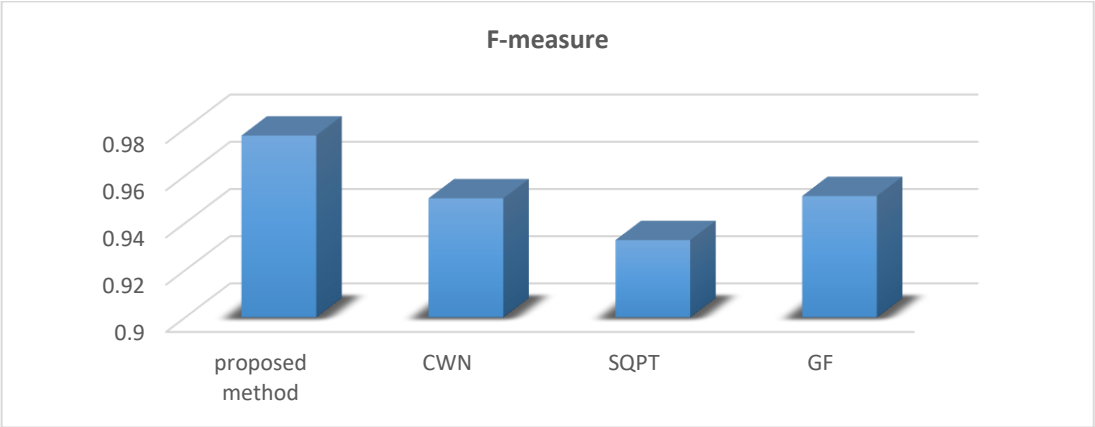

Figure 7. Comparing the F-measure of the proposed method and conventional methods

4. CONCLUSION

The problem studied in this research is the design of intrusion detection system using optimal perceptron and cuckoo algorithm. Common methods of intrusion detection systems have advantages of high accuracy in feature selection and automatic generation of optimal perceptron and disadvantages of not processing continuous data. that a new algorithm for intrusion detection was proposed and implemented, and the implementation results show the improvement of intrusion detection accuracy and compatibility with both continuous and discrete data types and the absence of additional overhead in processing continuous data in this system to select the set The reduced features are used by the cuckoo algorithm, then according to the frequency of different types of features in the intrusive and normal data, they are treated with the help of the optimal perceptron. The system is tested and the implementation results show a detection accuracy of 89.8%, which is a significant improvement over previous methods.

This work presents a new IDS based on the combination of neural network and cuckoo search optimization technique. Optimal perceptron for cuckoo classification and search is used to train neural network. Neural network training is done by updating the values of weights for better results. The proposed scheme is evaluated on the benchmark dataset of the IST Group from MIT Lincoln Laboratory under DARPA to identify normal and abnormal traffic. The evaluation criteria include accuracy, precision, intrusion detection rate, error warning rate, readability and F factor. The proposed method is also compared with the standard methods available in the literature, such as the method based on ad hoc wireless

networks [23] and the method based on quality of service and parallel technology [24] and the combined genetic and fuzzy method [25]. The simulation results, namely accuracy = 0.898, Precicion = 0.9341, False Posetive Rate = 0.0659, Recall = 0.9913, and F-measure = 0.977, clearly show the superior performance of the proposed method against the standard methods available in the literature.

REFERENCES

[1] Scarfone, Karen A., and Peter M. Mell. Guide to Intrusion Detection and Prevention Systems (IDPS)| NIST. No. Special Publication (NIST SP)-800-94. 2007.

[2] Sekar, Ramasubramanian, Ajay Gupta, James Frullo, Tushar Shanbhag, Abhishek Tiwari, Henglin Yang, and Sheng Zhou. ”Specification-based anomaly detection: a new approach for detecting network intrusions.” In Proceedings of the 9th ACM conference on Computer and communications security, pp. 265-274. ACM, 2002.

[3] Demuth, Howard B., Mark H. Beale, Orlando De Jess, and Martin T. Hagan. Neural network design. Martin Hagan, 2014.

[4] Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2018). A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection. Computers & Security, 75: p. 36-58.

[5] Chellam, A., Ramanathan, L., & Ramani, S. (2018). Intrusion detection in computer networks using lazy learning algorithm. Procedia computer science, 132: p. 928-936.

[6] Wang, C.-R., Xu, R.-F., Lee, S.-J., & Lee, C.-H. (2018). Network intrusion detection using equality constrained-optimization-based extreme learning machines. Knowledge-Based Systems, 147, 68-80.

[7] Ashfaq, R. A. R., Wang, X.-Z., Huang, J. Z., Abbas, H., & He, Y.-L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences, 378: p. 484-497 .

[8] Vishwakarma, S., Sharma, V., & Tiwari, A. (2017). An intrusion detection system using KNN-ACO algorithm. Int. J. Comput. Appl., 171(10), 18-23 .

[9] Amfo, J. K., & Hayfron-Acquah, J. B. (2018). Modeling of Hybrid Intrusion Detection System in Internet of Things using Support Vector Machine and Decision Tree. International Journal of Computer Applications, 181(15): p. 45-52.

[10] Li, W., Özcan, E., & John, R. (2017). Multi-objective evolutionary algorithms and hyper-heuristiالگوریتم فاخته for wind farm layout optimisation. Renewable Energy, 1 :p. 473-482 .

[11] F. Valeur, G. Vigna, C. Kruegel, R. Kemmerer, "Comprehensive approach to intrusion detection alert correlation", IEEE transaction on dependable and secure computing, 2008, pp. 146-169.

[12] S.J. Horng, M.Y. Su," A novel intrusion detection system based on hierarchical clustering and support vector machines", Expert systems with applications 38 ,2011, pp. 306–313.

[13] T. Chyssler, S.N. Tehrani, "Alarm reduction and correlation in defence of IP networks", Proceedings of the 13th International workshops on enabling technologies, IEEE computer society, 2008, pp. 229-234.

[14] Y. Gong, S. Mabo, C. Chen, "Intrusion detection system combining misuse detection and anomaly detection using genetic network programming", ICROS-SICE international joint conference, 2009, pp. 3463-3467.

[15] Y. Li, J .Xia, S. Zhang, " An efficient intrusion detection system based on support vector machines and gradually feature removal method", Expert systems with applications 39, 2012 pp. 424–430.

[16] Y.P. Zhou, " Hybrid model based on artificial immune system and PCA neural networks for intrusion detection", IEEE APCIP(Asian-pacific conference of information processing), 2009, pp. 21-24.

[17] Alazab M, Khurma RA, Awajan A, Camacho D. A new intrusion detection system based on moth–flame optimizer algorithm. Expert Syst Appl 2022;210:118439.

[18] Alzubi QM, Anbar M, Sanjalawe Y, Al-Betar MA, Abdullah R. Intrusion detection system based on hybridizing a modified binary grey wolf optimization and particle swarm optimization. Expert Syst Appl 2022;204:117597.

[19] Moutaz Alazab, Ruba Abu Khurma, Pedro A. Castillo, Bilal Abu-Salih, Alejandro Martín, David Camacho,An effective networks intrusion detection approach based on hybrid Harris Hawks and multi-layer perceptron,Egyptian Informatics Journal,Volume 25,2024,100423,ISSN 1110-8665,https://doi.org/10.1016/j.eij.2023.100423.

[20] Yang XS, Algorithms NI. Luniver Press. Beckington, UK; 242-6, 2008

[21] Hagan, M. T., H. B. Demuth, M. H. Beale, and O. De Jesús. ”Neural Network Design, 2nd Edtion.” Stillwater, Oklahoma. Oklahoma State University (2014).

[22] Gandomi AH, Yang X-S, Alavi AH (2013) Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems. Eng Comput 29(1):17–35

[23] Subba, Basant, Santosh Biswas, and Sushanta Karmakar. "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation." Engineering Science and Technology, an International Journal 19, no. 2 (2016): 782-799.

[24] Bul'ajoul, Waleed, Anne James, and Mandeep Pannu. "Improving network intrusion detection system performance through quality of service configuration and parallel technology." Journal of Computer and System Sciences 81, no. 6 (2015): 981-999.

[25] Elhag, Salma, Alberto Fernández, Abdullah Bawakid, Saleh Alshomrani, and Francisco Herrera. "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems." Expert Systems with Applications 42, no. 1 (2015): 193-202.

[26] Hajimirzaei, B., & Navimipour, N. J. (2019). Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. ICT Express, 5(1): p. 56-59