

Artificial Flora Optimization Algorithm with Functional Link Neural Network for DoS Attack Classification in WSN

Mahmoud A. Zaher[1,*], Mohmaed A. Labib[2]

[1] Faculty of Artificial Intelligence, Egyptian Russian University (ERU), Cairo, Egypt

[2 1] Faculty of Artificial Intelligence, Egyptian Russian University (ERU), Cairo, Egypt

Emails: Mahmoud.zaher@eru.edu.eg; m.labeeb85@yahoo.com

Abstract

Wireless sensor networks (WSN) is widely utilized for collecting data related to physical parameters from the environment. Security remains a challenging issue in the design of WSN. Security in WSN from Denial of Service (DoS) attack is an important security risk. This study introduces an artificial flora optimization algorithm with functional link neural network (AFOA-FLNN) model for DoS attack classification in WSN. The presented AFOA-FLNN model initially undergoes data pre-processing to transform the data into meaningful way. Secondly, the FLNN model is utilized for the effective recognition and classification of intrusions in WSN. Finally, the AFOA is exploited for optimally tuning the parameters involved in the FLNN model and results in enhanced performance. In order to demonstrate the better outcomes of the AFOA-FLNN model, a wide-ranging experimentation assessment on test data and the results pointed out the improved outcomes of the AFOA-FLNN model.

Keywords: DoS attack, Intrusion, Security, Machine learning, Parameter optimization, WSN

1. Introduction

Wireless sensor network (WSN) is guaranteed effective working with ongoing information handling in complex conditions. WSN is comprised of the nodes where nodes are associated with at least one a few sensor nodes. These nodes are utilized in numerous applications like observing climate conditions, production line execution, and persistent correspondence for military [1]. All these applications require node is more solid and steady. The life of the node has relied upon the battery force of node. In the event that the node consumes more battery power, the presentation of the organization is debasing. Sensor networks utilizing circulated remote innovation are used in numerous applications, for example, wellbeing observing framework, building or foundation access frameworks, debacle help, and wave cautioning frameworks [2]. A portion of these applications needs security because of asset requirements, in this manner, bringing about diminished Quality of Service (QoS). In asset obliged organizations, for example, WSN, conventional security plans can't be applied. Henceforth, need for new security measures to keep up with network usefulness without forfeiting execution turns into a need [3]. Figure 1 showcases the structure of WSN.

Energy utilization is a major question as the sensors are ordinarily minuscule and remote with restricted memory and usefulness giving way that the batteries(y) have a restricted power supply. Subsequently, challenges emerge during computation [4]. An organization or node can be impacted by numerous sorts of DoS attacks including those, constraining nodes to be out of gear or reserve mode. This influences the presentation of the node and the organization. In most pessimistic scenarios, the attacked node keeps on conveying to its neighbors lastly exhausts generally its power and pronounces itself dead, which decreases the organization's inclusion region [5]. Thus, WSN should be versatile with insignificant stand

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

by periods (network set up should be altered). The correspondence joins in such an eccentric climate (node disappointments) are kept utilitarian by applying a powerful steering calculation. In this paper, a clever methodology is proposed. The specialists utilize the sensor node's data to foresee or expect to stick attacks by utilizing key execution boundaries [6].

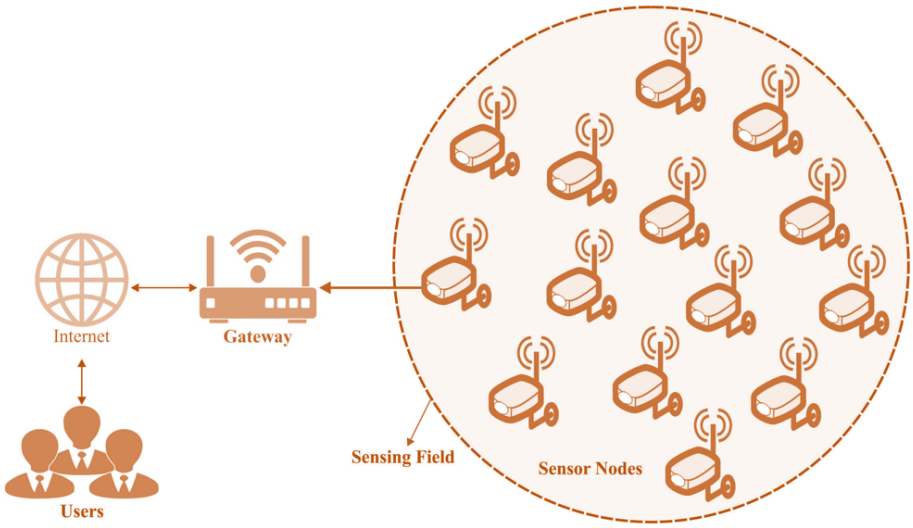


Figure 1. Structure of WSN

Denial of service (DoS) attack alludes to the utilization of client/server innovation to consolidate numerous PCs as an attack stage to send off attacks on at least one focus to expand the force of the attack [7]. Appropriated disavowal of-administration attack has changed the conventional shared attack mode, so there is no measurable rule for attack conduct, also, normal conventions and administrations are utilized in the attack. It is challenging to recognize attack or ordinary conduct just through the sorts of conventions and administrations. The conveyed refusal of administration attack isn't difficult to detect [8]. As of now, the examination on guard innovation against DDoS attacks at home and abroad is for the most part founded on the strategy for network interruption discovery. As indicated by the qualities of many-to-one attacks during the time spent DDoS attack, three characteristics [9] including the quantity of source IP addresses, the quantity of objective ports, and the stream thickness were utilized to depict the attributes of attack. These strategies can separate whether the greater part of the attack streams is objective, yet just utilize less message data, the majority of which just utilize the source IP address and objective port data, and cannot decide the particular attack type, so the identification rate isn't high. AI assumes a significant part in expectation. DDoS attack location in view of AI additionally has gained some headway. The AI calculations utilized for DDoS attack discovery primarily incorporate credulous Bayesian calculation stowed away Markov model and backing vector machine [10].

Security is a fundamental problem in wireless sensor networks of real time applications. The researchers in [11] aim are to introduce denial of service attack and responds to wireless sensor network for enhancing privacy by detection of the enemy. Distinct types of layer in the existence of WSN. These two kinds of ML techniques, NN, identify an SVM, a MAC layer attack. The researchers compared both technologies. The distributed attack is determined by the system that is attacked by attacker. This kind of attack causes additional problems in network function when compared to attacks included in a single node. Redemption of the system from the threat of DoS attack, an optimized ML approach should be developed in [12]. To identify DoS in WMSN an improved DNN approach has been introduced. The parameter needed is elected from adoptive PSO approach. The researches in [13] contain personalized data for intelligent underwater network.

This study introduces an artificial flora optimization algorithm with functional link neural network (AFOA-FLNN) model for DoS attack classification in WSN. The presented AFOA-FLNN model initially

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

undergoes data pre-processing to transform the data into meaningful way. Secondly, the FLNN model is utilized for the effective recognition and classification of intrusions in WSN. Finally, the AFOA is exploited for optimally tuning the parameters involved in the FLNN model and results in enhanced performance. In order to demonstrate the better outcomes of the AFOA-FLNN model, a wide-ranging experimental analysis is carried out on benchmark dataset.

2. The Proposed Model

In this study, a novel AFOA-FLNN model has been developed for DoS attack classification in WSN. The presented AFOA-FLNN model originally experiences data pre-processing to convert the data into meaningful way. Then, the FLNN model is utilized for the effective recognition and classification of intrusions in WSN. Lastly, the AFOA is exploited for optimally tuning the parameters involved in the FLNN model and results in enhanced performance.

2.1 FLNN based Classification

For DoS attack recognition and classification, the FLNN model is exploited. At addressing the problems compared with typical NN, the single layer NN (SLNN) was considered as alternative method [14]. But, the SLNN being linear by its nature one of the repeated fails to map the complex nonlinear problem. Thus, resolving challenges from single layer feed forward ANN is closely a complex task. In order to bridge the gap amongst the linearity in SLNN and very complex and estimation intensive MLNN, the FLNN infrastructure was projected [15]. The FLNN infrastructure employs an SLFF-NN to address the linear mapping. Consider that every element of input proposal beforehand expansion be signified as z(i),1 < i < d whereas every element z(i) was functionally extended as z_n (i),1 < n < N , Assume N = count of extended values for every input elements. An improvement of every input design was completed as:

$$x_1(i) = z(i), x_2(i) = f_1\big(z(i)\big), .., x_N(i) = f_N\big(z(i)\big) \quad (1)$$

Consider z(i),1 < i < d, d refers the set of features. This extended input design was later provided to SLNN and the network is trained to attain the selected output [16]. Figure 2 illustrates the structure of FLNN.

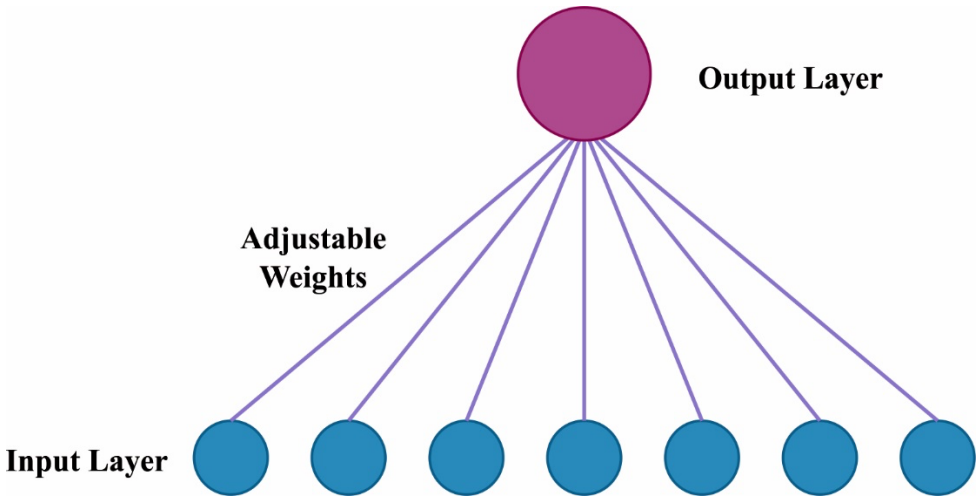


Figure 2. Process of FLNN

2.2 AFOA based Parameter Optimization

At the final stage, the AFOA is exploited for optimally tuning the parameters involved in the FLNN model and results in enhanced performance. The process of detection of an optimum survival position is employed in this method for discovery of an optimal solution subset of difficulties. The original plant, Offspring plant, plant place, and propagation distance are the 4 important components in AFOA approach. Evolution, selection, and Spreading behaviors are 3 most important behavioural patterns. Each plant location represents to solution, and fitness of the position is exploited for representing the solution quality. At first, this technique generates the original plant at random. Finally, roulette is employed to

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

decide survival seed. Survival seed becomes an original plant. Frequently iterated until the termination condition is met. This technique comprises exterior documents for saving the finest solution [17].

Initialization

All the decision parameters of testing function functioned in our work comprise lower limit $\vec{X}^{min} = [X^{\min}, X^{\min}, \ldots, X_D^{\min}]^T$ and upper limit $\vec{X}^{max} = [X_1^{\max}, X_2^{\max}, \ldots, X_D^{\max}]^T$. Firstly, this technique produces N original plants according to lower and upper limits of the decision parameters. This technique exploits i rows and j columns matrix P_{ij} for denoting the position of original plant, in which $i = 1,2, \ldots, D$ represents the dimension, $j = 1,2, \ldots, N$ denotes the amount of original plant:

$$P_{ij} = rand(0,1) \cdot (X_i^{\max} - X_i^{mm}) + X_i^{min} \quad (2)$$

Now, $rand(0,1)$ represents the arbitrary number within [0,1].

Evolution Behavior

The original plant spread offspring to a particular range with radius viz. grandparent plant, propagation distance, and novel propagation distance imitates the propagation distance of parent [18]:

$$d_j = d_{lj} \cdot rand(0,1) \cdot c_1 + d_{2j} \cdot rand(0,1) \cdot c_2 \quad (3)$$

Here c_1 & c_2 indicates learning coefficient, d_{lj} and d_{2j} signifies propagation distance of grandparent and parent plants, rand $(O,1)$ shows arbitrary distribution number within [0,1]. The parent propagation distance becomes a novel grandparent propagation distance:

$$d'_{1j} = d_{2j} \quad (4)$$

The standard AF optimization technique employs SD amongst the location of the original plant and offspring plant as novel parent propagation distance:

$$d'_{2j} = \sqrt{\sum_{i=1}^{N} (P_{ij} - P'_{ij})^2 / N} \quad (5)$$

To remember the data of an ideal solution, AFO optimization method employs plants from the exterior document. The novel parent propagation distance is the variation amongst the location of plant in exterior documents $P^*_{i_d}$ and offspring plant P'_{i_d}:

$$d'_{2j} = P^*_{ij} - P'_{ij} \quad (6)$$

Spreading Behavior

This method generates offspring plant according to the novel propagation distance and original plant location:

$$P'_{i,j \cdot b} = G_{i,j \cdot b} + P_{\mathrm{i,j}} \quad (7)$$

Now $b = 1,2, \ldots, B$, B characterizes quantity of offspring plant that one original plant might propagate, $P'_{i,j \cdot b}$ characterizes place of offspring plant, $P_{\mathrm{i,j}}$ shows place of original plant, $G_{i,j \cdot b}$ characterizes arbitrary value with Gaussian distribution using mean 0 & variance j. Produce novel original plant that there are no offspring plant lives.

Select Behavior

In typical AF system, the survival possibility describes the offspring plant endured. It can be shown in the following:

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

$$p = \left|\sqrt{F\left(P'_{i,j\cdot b}\right)/F_{max}}\right| \cdot Q_x^{(j\cdot b-1)}. \quad (8)$$

Now Q_X is electing possibility range within [0,1]. $F_{\max}$ represents fitness of offspring plant with maximal fitness. $F(P'_{i,j\cdot b})$ represents fitness of $(j \cdot b)th$ solution. The assessment equation of fitness is the process of objective problem. In AFO technique, the Pareto dominance relation has been employed. It can be shown in the following:

$$p = 0.9 \cdot \frac{domi(j \cdot b)}{B} + 0.1 \quad (9)$$

In which domi $(j \cdot b)$ represents amount of the solution that subjects with solution $(j \cdot b)$. B symbolizes the amount of offspring plant that one original plant might propagate.

3. Results and Discussion

In this section, a brief experimental validation process is carried out using three benchmark datasets. The dataset details are given in Table 1.

Table 1 Dataset details

Class Labels	Dataset 1	Dataset 2	Dataset 3
Normal	184343	120223	24025
Attacked	21461	13160	3568
Total	205804	133383	27593

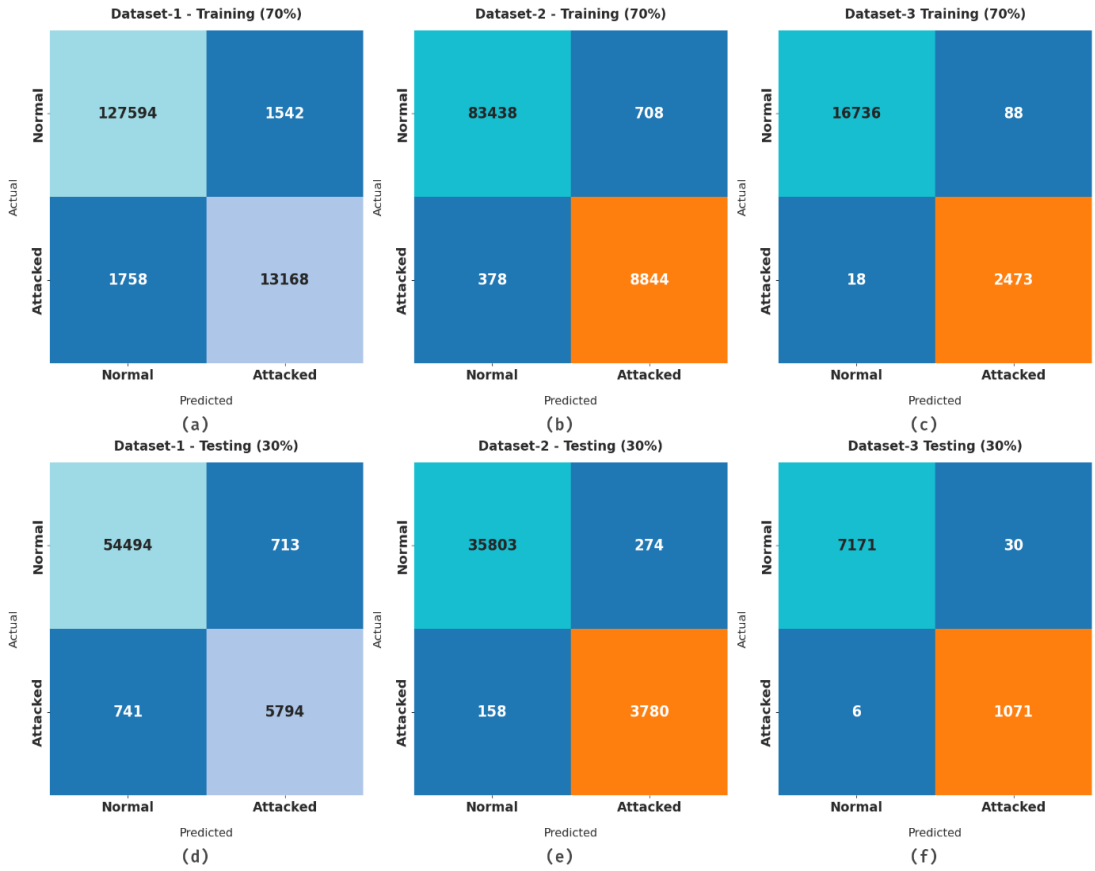


Figure 3. Confusion matrix of AFOA-FLNN technique

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

Figure 3 shows the confusion matrices produced by the AFOA-FLNN model. With 70% of training set on dataset-1, the AFOA-FLNN model has identified 127594 samples into normal and 13168 samples into attacked. Also, with 70% of training set on dataset-2, the AFOA-FLNN approach has identified 83438 samples into normal and 8844 samples into attacked. In line with, with 70% of training set on dataset-3, the AFOA-FLNN system has identified 16736 samples into normal and 2473 samples into attacked. At the same time, with 30% of testing set on dataset-1, the AFOA-FLNN algorithm has identified 54494 samples into normal and 5794 samples into attack. Moreover, with 30% of testing set on dataset-2, the AFOA-FLNN technique has identified 35803 samples into normal and 3780 samples into attacked. Furthermore, with 30% of testing set on dataset-3, the AFOA-FLNN methodology has identified 7171 samples into normal and 1071 samples into attacked.

Table 2 Result analysis of AFOA-FLNN technique under 70% of training dataset

Training (70%)				
Class Labels	**Accuracy**	**Precision**	**Recall**	**F-Score**
Dataset-1				
Normal	97.71	98.64	98.81	98.72
Attacked	97.71	89.52	88.22	88.86
Average	**97.71**	**94.08**	**93.51**	**93.79**
Dataset-2				
Normal	98.84	99.55	99.16	99.35
Attacked	98.84	92.59	95.9	94.22
Average	**98.84**	**96.07**	**97.53**	**96.78**
Dataset-3				
Normal	99.45	99.89	99.48	99.68
Attacked	99.45	96.56	99.28	97.90
Average	**99.45**	**98.23**	**99.38**	**98.79**

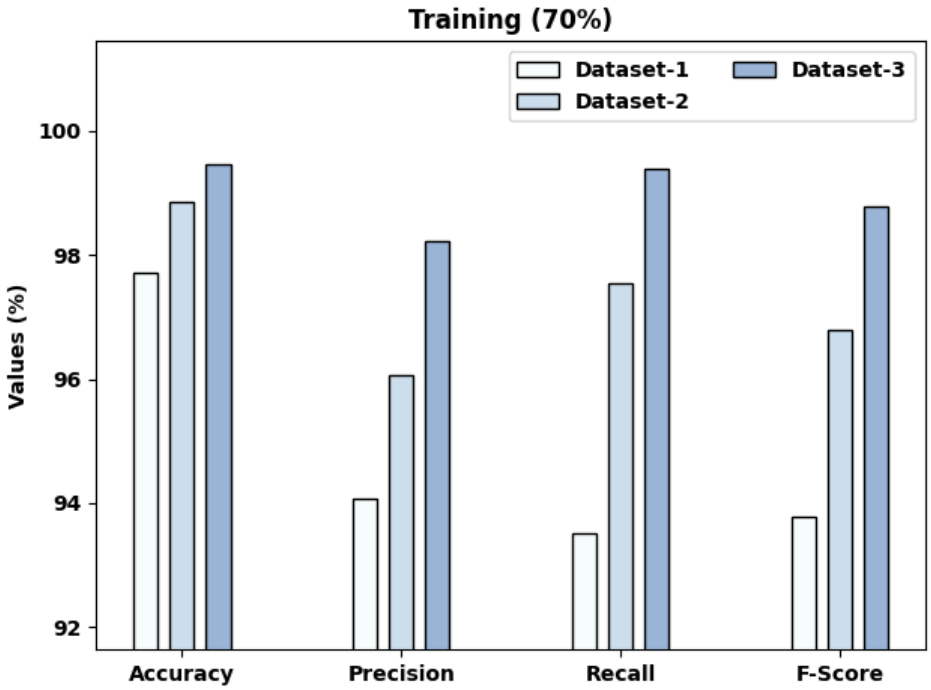


Figure 4. Result analysis of AFOA-FLNN technique under 70% of training dataset

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

Table 2 and Figure 4. provide a detailed result analysis of the AFOA-FLNN model on 70% of training dataset. The experimental values indicated that the AFOA-FLNN model has reached effectual DoS attack classification performance. On applied dataset-1, the AFOA-FLNN model has resulted in average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 97.71%, 94.08%, 93.51%, and 93.79% respectively. Along with that, on applied dataset-2, the AFOA-FLNN approach has resulted in average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.84%, 96.07%, 97.53%, and 96.78% correspondingly. In line with, on applied dataset-3, the AFOA-FLNN technique has resulted in average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.45%, 98.23%, 99.38%, and 98.79% correspondingly.

Table 3 Result analysis of AFOA-FLNN technique under 30% of testing dataset

Testing (30%)				
Class Labels	**Accuracy**	**Precision**	**Recall**	**F-Score**
Dataset-1				
Normal	97.65	98.66	98.71	98.68
Attacked	97.65	89.04	88.66	88.85
Average	**97.65**	**93.85**	**93.68**	**93.77**
Dataset-2				
Normal	98.92	99.56	99.24	99.40
Attacked	98.92	93.24	95.99	94.59
Average	**98.92**	**96.40**	**97.61**	**97.00**
Dataset-3				
Normal	99.57	99.92	99.58	99.75
Attacked	99.57	97.28	99.44	98.35
Average	**99.57**	**98.60**	**99.51**	**99.05**

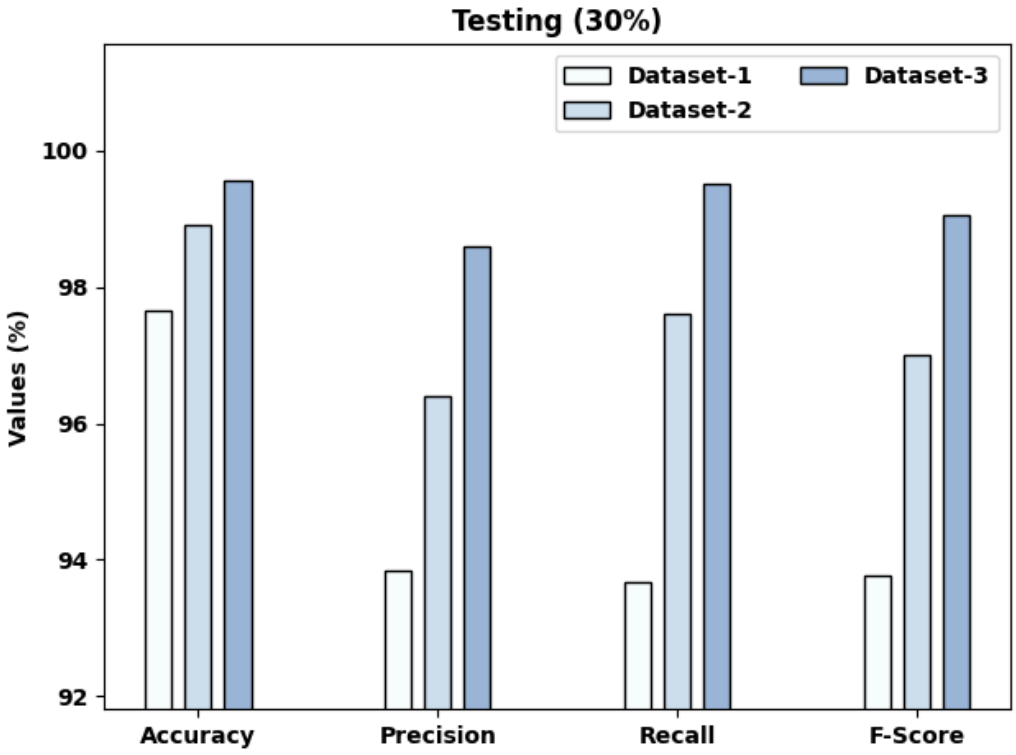


Figure 5. Result analysis of AFOA-FLNN technique under 30% of testing dataset

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

Table 3 and Figure 5 offer a detailed result analysis of the AFOA-FLNN system on 30% of testing dataset. The experimental values exposed that the AFOA-FLNN method has reached effectual DoS attack classification performance. On applied dataset-1, the AFOA-FLNN model has resulted in average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 97.65%, 92.85%, 93.68%, and 93.77% correspondingly. Likewise, on applied dataset-2, the AFOA-FLNN model has resulted in average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.92%, 96.40%, 97.61%, and 97% correspondingly. Eventually, on applied dataset-3, the AFOA-FLNN model has resulted in average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.57%, 98.60%, 99.51%, and 99.05% correspondingly.

Table 4 Accuracy analysis of AFOA-FLNN technique with existing methods under three datasets

Accuracy (%)			
Methods	**Dataset-1**	**Dataset-2**	**Dataset-3**
KNN Algorithm	96.53	96.53	97.93
LOR Algorithm	94.42	98.33	96.53
Support Vector Machine Model	92.31	85.29	83.89
Gboost Algorithm	95.58	97.58	97.93
Decision Tree Algorithm	96.63	97.23	94.07
Naïve Bayes Algorithm	81.78	97.23	94.07
LSTM Model	95.12	97.93	96.88
MLP Algorithm	96.88	98.28	96.88
AFOA-FLNN	97.65	98.92	99.57

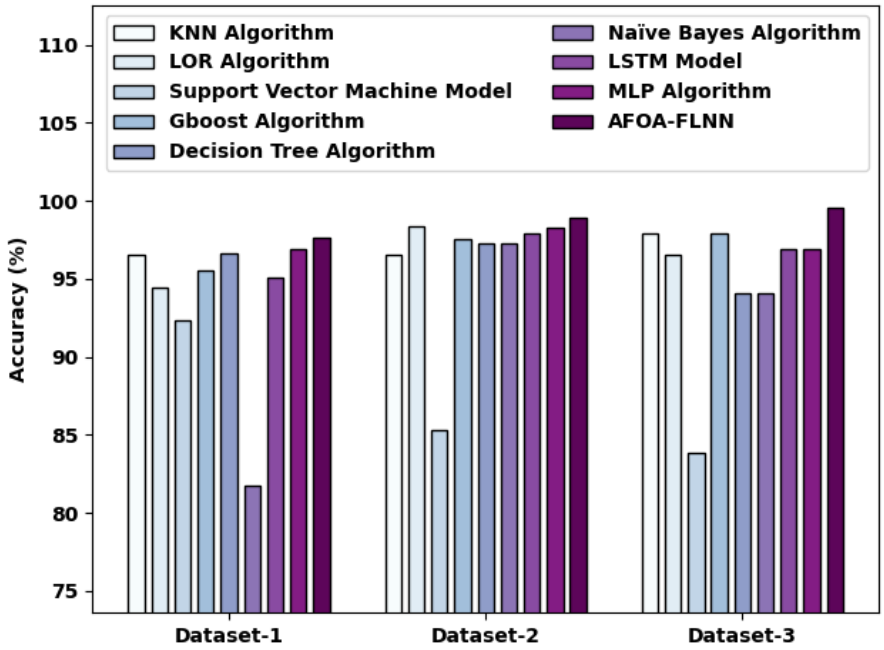


Figure 6. Accuracy analysis of AFOA-FLNN technique with existing methods

Table 4 and Figure 6 highlight the comparative accuracy examination of the AFOA-FLNN model on three datasets [19]. The results implied that the AFOA-FLNN model has gained effective performance with maximum accuracy values on each dataset. For instance, with dataset-1, the AFOA-FLNN model has offered higher accuracy of 97.65% whereas the KNN, LOR, SVM, Gboost, DT, NB, LSTM, and MLP models have obtained 96.53%, 94.42%, 92.31%, 95.58%, 96.63%, 81.78%, 95.12%, and 96.88%. Moreover, with dataset-2, the AFOA-FLNN model has offered higher accuracy of 98.92% whereas the KNN, LOR, SVM, Gboost, DT, NB, LSTM, and MLP algorithms have obtained 96.53%, 98.33%,

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

85.29%, 97.58%, 97.23%, 97.23%, 97.93%, and 98.28%. In line with, with dataset-3, the AFOA-FLNN system has offered higher accuracy of 99.57% whereas the KNN, LOR, SVM, Gboost, DT, NB, LSTM, and MLP techniques have reached 97.93%, 96.53%, 83.89%, 97.93%, 94.07%, 94.07%, 96.88%, and 96.88%.

Table 5 F-score analysis of AFOA-FLNN technique with existing methods under three datasets

F-Score (%)			
Methods	**Dataset-1**	**Dataset-2**	**Dataset-3**
KNN Algorithm	90.15	92.71	95.28
LOR Algorithm	82.82	91.61	89.05
Support Vector Machine Model	61.56	79.88	92.71
Gboost Algorithm	92.91	96.38	96.38
Decision Tree Algorithm	91.28	96.11	97.11
Naïve Bayes Algorithm	57.52	87.95	83.55
LSTM Model	80.98	91.98	87.58
MLP Algorithm	79.88	92.35	89.05
AFOA-FLNN	93.77	97.00	99.05

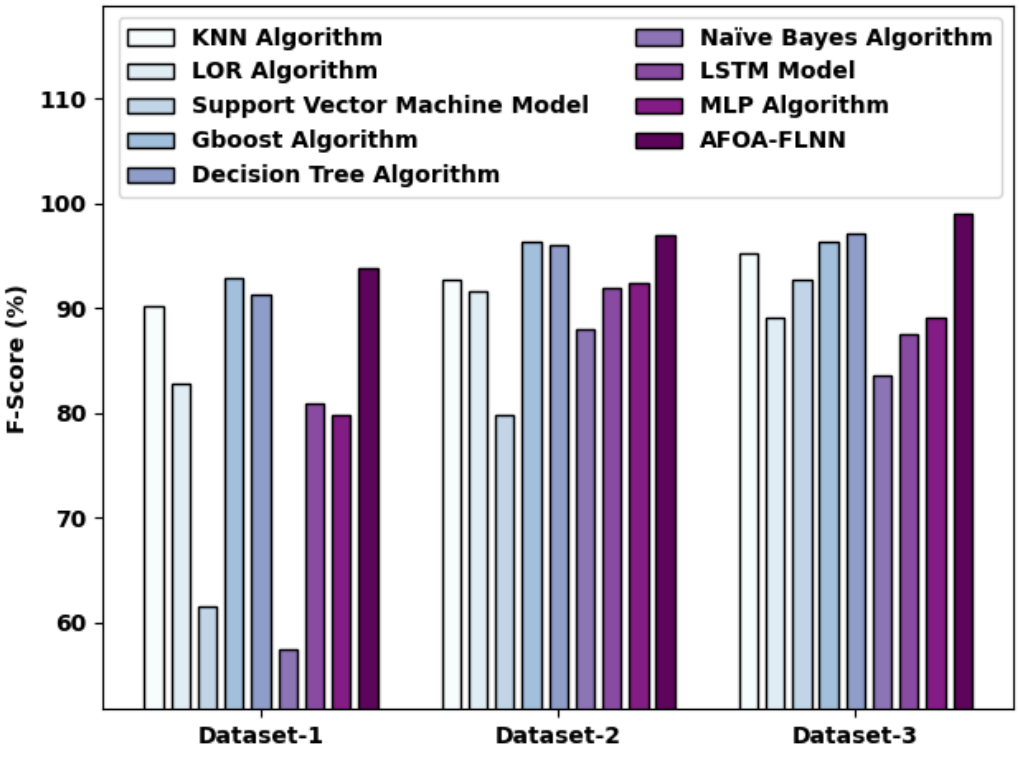


Figure 7. F-score analysis of AFOA-FLNN technique with existing methods

Table 5 and Figure 7 examine the comparative F-score analysis of the AFOA-FLNN model on three datasets. The outcomes revealed that the AFOA-FLNN model has gained effective performance with maximal F-score values on each dataset. For instance, with dataset-1, the AFOA-FLNN model has offered higher F-score of 93.77% whereas the KNN, LOR, SVM, Gboost, DT, NB, LSTM, and MLP models have obtained 90.14%, 82.82%, 61.56%, 92.91%, 91.28%, 57.52%, 80.98%, and 78.88%. Furthermore, with dataset-2, the AFOA-FLNN model has accessible maximum F-score of 97% whereas

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

the KNN, LOR, SVM, Gboost, DT, NB, LSTM, and MLP techniuqes have obtained 92.71%, 91.61%, 79.88%, 96.38%, 96.11%, 87.95%, 91.98%, and 92.35%. Also, with dataset-3, the AFOA-FLNN approach has obtainable supeiror F-score of 99.05% whereas the KNN, LOR, SVM, Gboost, DT, NB, LSTM, and MLP approaches have reached 95.28%, 89.05%, 92.71%, 96.38%, 97.11%, 83.55%, 87.58%, and 89.05%.

4. Conclusion

In this study, a novel AFOA-FLNN model has been developed for DoS attack classification in WSN. The presented AFOA-FLNN model originally experiences data pre-processing to convert the data into meaningful way. Then, the FLNN model is utilized for the effective recognition and classification of intrusions in WSN. Lastly, the AFOA is exploited for optimally tuning the parameters involved in the FLNN model and results in enhanced performance. In order to demonstrate the better outcomes of the AFOA-FLNN model, a wide-ranging experimental analysis is carried out on benchmark dataset and the results pointed out the improved outcomes of the AFOA-FLNN model. Thus, the AFOA-FLNN model has been utilized for the recognition and classification of DoS attacks in WSN. In future, the detection rate of the AFOA-FLNN model can be enhanced by feature selection models.

References

[1] Arjunan, S. and Sujatha, P., 2018. Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. Applied Intelligence, 48(8), pp.2229-2246.

[2] Arjunan, S. and Pothula, S., 2019. A survey on unequal clustering protocols in wireless sensor networks. Journal of King Saud University-Computer and Information Sciences, 31(3), pp.304-317.

[3] Arjunan, S., Pothula, S. and Ponnurangam, D., 2018. F5N-based unequal clustering protocol (F5NUCP) for wireless sensor networks. International Journal of Communication Systems, 31(17), p.e3811.

[4] Famila, S., Jawahar, A., Sariga, A. and Shankar, K., 2020. Improved artificial bee colony optimization based clustering algorithm for SMART sensor environments. Peer-to-Peer Networking and Applications, 13(4), pp.1071-1079.

[5] Premkumar, M. and Sundararajan, T.V.P., 2021. Defense countermeasures for DoS attacks in WSNs using deep radial basis networks. Wireless Personal Communications, 120(4), pp.2545-2560.

[6] Chen, H., Meng, C., Shan, Z., Fu, Z. and Bhargava, B.K., 2019. A novel Low-rate Denial of Service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang Transformation and Trust Evaluation. IEEE Access, 7, pp.32853-32866.

[7] Almomani, I.M. and Alenezi, M., 2018. Efficient Denial of Service Attacks Detection in Wireless Sensor Networks. J. Inf. Sci. Eng., 34(4), pp.977-1000.

[8] Premkumar, M. and Sundararajan, T.V.P., 2020. DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocessors and Microsystems, 79, p.103278.

[9] Islam, M.N.U., Fahmin, A., Hossain, M. and Atiquzzaman, M., 2021. Denial-of-service attacks on wireless sensor network and defense techniques. Wireless Personal Communications, 116(3), pp.1993-2021.

[10] Segura, G.A.N., Skaperas, S., Chorti, A., Mamatas, L. and Margi, C.B., 2020, June. Denial of service attacks detection in software-defined wireless sensor networks. In 2020 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-7). IEEE.

[11] Yu, D., Kang, J. and Dong, J., 2021. Service attack improvement in wireless sensor network based on machine learning. Microprocessors and Microsystems, 80, p.103637.

[12] Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Basha, A.R. and Jayasankar, T., 2021. An optimized deep neural network based DoS attack detection in wireless video sensor network. Journal of Ambient Intelligence and Humanized Computing, pp.1-14.

[13] Ahmad, B., Jian, W., Enam, R.N. and Abbas, A., 2021. Classification of DoS attacks in smart underwater wireless sensor network. Wireless Personal Communications, 116(2), pp.1055-1069.

[14] Al-Ahmadi, S., 2021. Performance evaluation of machine learning techniques for DOS detection in wireless sensor network. International Journal of Network Security & Its Applications (IJNSA) Vol, 13.

[15] Katuwal, R. and Suganthan, P.N., 2019. Stacked autoencoder based deep random vector functional link neural network for classification. Applied Soft Computing, 85, p.105854.

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022

[16] Naik, B., Obaidat, M.S., Nayak, J., Pelusi, D., Vijayakumar, P. and Islam, S.H., 2019. Intelligent secure ecosystem based on metaheuristic and functional link neural network for edge of things. IEEE Transactions on Industrial Informatics, 16(3), pp.1947-1956.
[17] Cheng, L., Wu, X.H. and Wang, Y., 2018. Artificial flora (AF) optimization algorithm. Applied Sciences, 8(3), p.329.
[18] Bacanin, N., Tuba, E., Bezdan, T., Strumberger, I. and Tuba, M., 2019, November. Artificial flora optimization algorithm for task scheduling in cloud computing environment. In International Conference on Intelligent Data Engineering and Automated Learning (pp. 437-445). Springer, Cham.
[19] Wazirali, R., Ahmad, R. (2022). Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime. CMC-Computers, Materials & Continua, 70(3), 4922–4946.

DOI: https://doi.org/10.54216/IJWAC.040101
Received: November 12, 2021 Accepted: January 22, 2022