International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8093
***Article Received:** 24 June 2023 **Revised:** 23 August 2023 **Accepted:** 06 September 2023*

DDoS Attack Detection in WSN using Modified Invasive Weed Optimization with Extreme Learning Machine

[1,*]C. Murugesh, [2]Dr. S. Murugan
[1]Assistant Professor/Programmer, Department of Computer and Information Science,
Annamalai University, Annamalai Nagar.
78murugesh@gmail.com
[2]Assistant Professor, Dr. M.G.R. Government Arts and Science College for Women,
Villupuram.
smuruganmpt79@gmail.com

Abstract—Wireless sensor networks (WSN) are the wide-spread methodology for its distribution of the vast amount of devoted sensor nodes (SNs) that is employed for sensing the atmosphere and gather information. The gathered information was transmitted to the sink nodes via intermediate nodes. Meanwhile, the SN data are prone to the internet, and they are vulnerable to diverse security risks, involving distributed denial of service (DDoS) outbreaks that might interrupt network operation and compromises data integrity. In recent times, developed machine learning (ML) approaches can be applied for the discovery of DDoS attacks and accomplish security in WSN. To achieve this, this study presents a modified invasive weed optimization with extreme learning machine (MIWO-ELM) model for DDoS outbreak recognition in the WSN atmosphere. In the presented MIWO-ELM technique, an initial stage of data pre-processing is conducted. The ELM model can be applied for precise DDoS attack detection and classification process. At last, the MIWO method can be exploited for the parameter tuning of the ELM model which leads to improved performance of the classification. The experimental analysis of the MIWO-ELM method takes place using WSN dataset. The comprehensive simulation outputs show the remarkable performance of the MIWO-ELM method compared to other recent approaches.

Keywords- Wireless sensor networks; DDoS attack; Machine learning; Metaheuristics; Extreme learning machine.

I. INTRODUCTION

WSN is built on device network, which provides a potentially sustainable and green solution for expanding data collected in a specific environment and delivering it to the end user. WSN is a robust and effective infrastructure-free network made up of tens to vast numbers of low-power detectors that are organised haphazardly [1]. These devices can take feedback from the environment, analyze it, and then communicate it. Sensors are disseminated indiscriminately or purposefully on external surroundings, acting as the sensing layer of IoT devices, and have a wide range of applications [2]. WSNs are commonly used in non-military and military activities to instrument, observe, and respond to an occurrence at a remote or inaccessible location. One of the aims of modern education is to cultivate autonomous learning abilities and lifelong learning abilities [3]. A WSN deploys several SNs inside or around the specified zone. The sensors may be put in any order and do not require any pre-planning, making them ideal for tough and unaccepting landscapes. Magnetic sensors, seismic sensors, thermal sensors, acoustic sensors, infrared sensors, and other types of sensors are used in WSN clusters [4]. SNs are important for sensing locations and events, as well as for continually monitoring any region. SNs have a wide range of applications and can be quite useful in a variety of industries.

With the advent of wireless transmission, mobile sensor networking has recently piqued the interest of both industry and academic researchers interested in real-time solutions [5]. WSN is a network of specialised SNs scattered across space that monitor and capture actual environmental factors before organising the data at a centralised location [6]. WSNs detect and record environmental factors such as sound, humidity, levels of pollution, surf, rain, etc. WSNs are used in challenging and hazardous environments where wired networks cannot be installed, and they are beneficial in circumstances where physically collecting the data that the sensors can gather would be impossible or dangerous for a person [7]. A sensing unit, a power supply, a radio transmitting arrangement, a peripheral device, and data storage tools are all included in a WSN sensor. These components are built using limited resources, such as computing power and processing capability. As a result, sensor energy conservation is a difficult issue that has to be investigated further in order to extend the network's lifetime [8].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8093
***Article Received:** 24 June 2023 **Revised:** 23 August 2023 **Accepted:** 06 September 2023*

WSNs are prone to attacks and security threats. Securing them becomes a challenge as their limited resources like communication bandwidth, battery power, storage space, processing capabilities, and memory. Moreover, because of their deployment in unsupervised environment, SNs are visible to physical outbreaks [9]. Most prevalent and frequent types of outbreaks against WSN is DoS attack. They come in various forms in order to drain the node sources, particularly the energy and its capability to execute other duties. Later, certain security systems are essential for protecting WSNs from DoS attacks [10]. Various studies have devised various intrusion detection systems (IDS) helps to find such security attacks. Deep learning (DL) and ML approaches are utilized in numerous studies and have frequently shown higher levels of precision.

This study presents a modified invasive weed optimization with extreme learning machine (MIWO-ELM) technique for DDoS outbreak recognition in the WSN atmosphere. In the presented MIWO-ELM technique, an initial stage of data pre-processing is conducted. The ELM approach can be applied for accurate DDoS attack detection and classification process. At last, the MIWO approach can be exploited for the tuning process of the ELM method which leads to improved performance of the classification. The experimental analysis of the MIWO-ELM method occurs by employing WSN dataset.

II. RELATED WORKS

In [11], devised fractional anti-corona virus optimization (FACVO) related deep neuro-fuzzy network (DNFN) to recognize DDoS in the cloud. The processing stages involved in DDoS attack detection are creation of data augmentation, feature fusion, log files, and DDoS outbreak recognition. The feature fusion was performed by deep QNN (DQNN) and RV coefficient, and the data augmentation was effectuated. Next, the fractional calculus (FC) and ACVO approach are combined to make the FACVO method. The presented DNFN was given training using the FACVO method that recognizes the DDoS attacks. Kadam and Krovi [12] projected a new hybrid KSVM technique that depends on SVM and KNN system to frame a secure architecture to discover Distributed DoS attacks which is the part of ML method.

Al-Hadhrami and Hussain [13] devised an ML structure for finding DDoS outbreaks in IoT networking system. This structure collects and examines IoT traffic by putting it under ML method for identifying attacks. In [14], proposed a novel DL-based Defense Mechanism (DLDM) method, lightweight DoS detection scheme has to separate and spot the outbreaks in data forwarding phase (DFP). This research described the novel method for the effective identification of DoS outbreaks like homing, exhaustion, flooding, and jamming. The author conducted wide experiments that can precisely separate adversary and it is resilient to DoS attack. Mhamdi et al. [15] presented a fusion unsupervised DL technique with the use of the SAE and 1-class SVM (SAE-1SVM) for DDoS attack detection.

Sait et al. [16] design a heuristic feature selection with DL-related DDoS (HFSDL-DDoS) outbreak recognition method in WSNs. The projected method means to classify and recognize occurrence of DDoS attacks in WSN. As well, to improve the detection performance, the presented method includes the immune clonal GA (ICGA) related feature selection (FS) method. Besides, a fruit fly algorithm (FFA) with BiLSTM based classification method was used. Zhou et al. [17] devise an ML related online monitoring of internet traffic mechanism utilizing a stream processing related big data structure and spark streaming, to find DDoS outbreaks in real world. The mechanism has stream processor, collector, and messaging mechanism. The author exploits a correlation-related feature selection approach and chooses 4 essential networking factors in ML-related DDoS detection method.

III. THE PROPOSED MODEL

In this research, a novel MIWO-ELM methodology for accurate and automated recognition of DDoS outbreaks in the WSN atmosphere. The suggested MIWO-ELM methodology comprises three main procedures like data normalization, ELM based DDoS outbreak recognition, and MIWO based tuning process. Fig. 1 illustrates the work flow of MIWO-ELM method.

A. Data Pre-processing

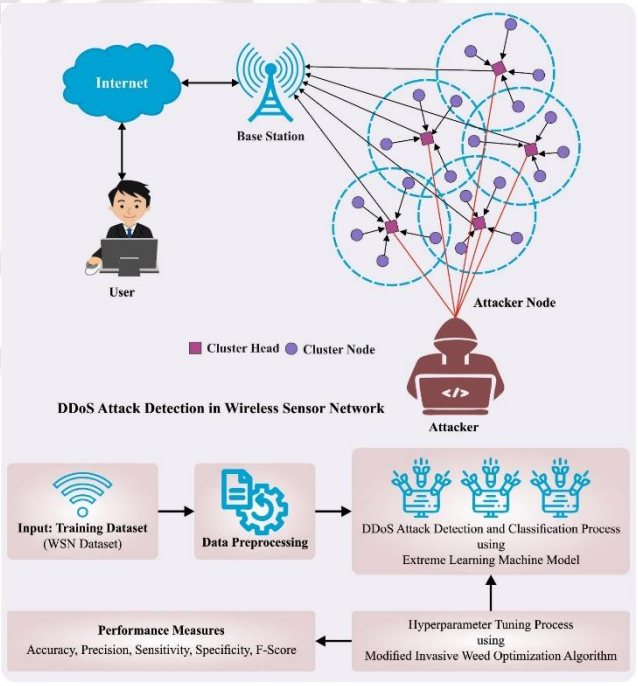

Figure 1. Fig. 1 Overall flow of MIWO-ELM approach

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8093
***Article Received:** 24 June 2023 **Revised:** 23 August 2023 **Accepted:** 06 September 2023*

In this MIWO-ELM method, an initial stage of data pre-processing is carried out. Min-max normalization method is used for scaling normalized attribute value within [0, 1] to accomplish uniformity in the value of the data feature [18]. The successive Eq. (1) is employed for standardizing data factor value in a particular limit.

$$\text{Min Max} = \frac{X_i - \min(A)}{\max(A) - \min(A)} \quad (1)$$

B. ELM based DDoS Attack Detection Model

For accurate DDoS attack detection and classification processes, the ELM can be applied. Here, the ELM is utilized as the classifier of label layer. The ELM unlike the gradient-based algorithm features the random series of parameters of HL nodes and the only computation of the output weight [19]. The study presents a Non-linearity into the system due to the nonlinear activation function in the HL. Thus, the ELM converge faster than the classical approach. Simultaneously, random HLs assurance the global approximation capability. Fig. 2 depicts the infrastructure of ELM.

In the training of ELM, dissimilar sets of input and output (x_j, t_i) are needed. Where $\chi_j = [x_{i1}, x_{i2}, \dots, x_{in}]^T \in R^n$, $t_i = [t_{i1}, t_{i2}, \dots, t_{im}]^T \in R^m$. The ELM module with the amount of HL nodes L is formulated as follows:

$$\sum_{i=1}^{L} \beta_i \, h(\omega_i \cdot x_j + b_i) = O_j \quad (2)$$

In Eq. (2), $h(x)$ denotes the activation function of the HL which gives nonlinearity for the system. $\omega_i = [\omega_{i1}, \omega_{i2}, \dots, \omega_{in}]^T$ shows the input weight matrix. β_i represents the output weight matrix. b_j refers to the HL bias. O_j indicates the output of model.

The objective of ELM training is to minimalize the error that is given below:

$$\sum_{j=1}^{N} ||O_j - t_j|| = 0 \quad (3)$$

The target matrix T is formulated as follows:

$$H\beta = T \quad (4)$$

$$H = \begin{bmatrix} h(\omega_{11}x + b_1) & \dots & h(\omega_L \cdot x_L + b_L \\ \vdots & \ddots & \vdots \\ h(\omega_1 \cdot x_N + b_1) & \dots & h(\omega_L \cdot x_N + b_L) \end{bmatrix} \quad (5)$$

In the formula, H indicates the output of HL nodes. β denotes the output weight matrix. T shows the target matrix. During the classical gradient-based training, each parameter of the network is generally adjusted while ELM need to define the input weight of random parameter ω_i and the HL bias b_j. The output matrix of HLs and the output weight β can be evaluated. Thus, the learning method of ELM network is a system of linear equation resolving:

$$\beta' = H^+ T \quad (6)$$

In Eq. (18), H^+ represents the MoorePenrose generalized inverse matrix of H.

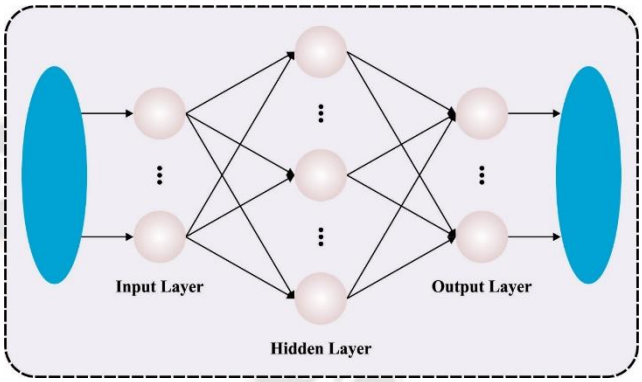

Figure 2. Architecture of ELM

C. Parameter Tuning using MIWO Algorithm

At last, the MIWO algorithm can be utilized for the parameter tuning of the ELM model. IWO algorithm is a population based stochastic optimization method motivated by the behaviors of weed colonization [20]. Compared to other algorithms, MIWO is utilized in various applications of Engineering and Sciences, due to its prominent features including spatial dispersal, competitive exclusion, and reproduction. The subsequent steps included in MIWO are given below:

Step 1: Initialization: A limited amount of population is arbitrarily produced over the search space.

Step 2: Reproduction: Based on its relative worst and best fitness values, all the candidate weeds of the populace is capable of generating fresh weeds of candidate weed after getting into the blooming tree. It declined linearly from the $(S_{\max})$ maximum weed to $(S_{\min})$ minimal weeds with $S_{\min}$ for the worst candidate weed, $S_{\max}$ for the fittest candidate weed in the population.

$$n(w_i) = \frac{S_{\max}\left(fit_{\max} - fit(w_i)\right) + S_{\min}(fit(w_i) - fit_{\min})}{fit_{max} - fit_{min}} \quad (7)$$

In Eq. (7), $fit_{\max}$ and $fit_{\min}$ indicates the maximal and minimal fitness values of the population, correspondingly. $n(w_i)$ denotes the number of seeds produced of i^{th} weeds, $S_{\max}$ and $S_{\min}$ are predetermined parameters. $fit(w_i)$ shows the fitness value of i^{th} weeds.

Step 3: Spatial Distribution: The fresh weeds are dispersed uniformly over the search space with the varying standard

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8093
***Article Received:** 24 June 2023 **Revised:** 23 August 2023 **Accepted:** 06 September 2023*

deviation and mean of parent weed location, described as follows:

$$\sigma_{gen} = \frac{(gen_{\max} - gen)^{mi}}{gen_{\max}^{mi}}(\sigma_{\max} - \sigma_r) + \sigma_r \qquad (8)$$

In Eq. (8), $gen_{\max}$ shows the maximal generation, σ_{gen} shows the standard deviation (SD) at the current generation. mi indicates the non-linear modulation index and necessity of mi are produced seeds can be closer to the parent weeds.$\sigma_{\max}$ and σ_r represent the maximum and minimum SDs, predetermined parameters.

Step 4: Competitive Segregation: When the plant doesn't leave any progeny, then it can be extinguished, or else it takes over the world. If the number of parental weeds and the freshly produced weed exceed the maximal limit ($W_{\max}$), the weed with worst fitness values is detached to $W_{\max}$ from the populace.

Step 5: Terminating Criteria:

(1) The existing iteration is equivalent to the upper boundary of the iteration amount.

(2) The above-mentioned procedures (Steps 1-4) attained the maximal amount of fitness values.

(3) $|f(X^*) - f(x)| \leq \varepsilon$ where x^* denotes the fittest solution, x denotes the better solution and ε indicates the smaller tolerance value. When the procedures (Steps 1- 4) attain the above-mentioned condition, the process will stop.

In IWO algorithm, the Gaussian function is utilized. Based on the Gauss distribution (GD) of arbitrary variables, it generates offspring for the IWO reproduction mode. The Cauchy distribution (CD) function gives best outcomes rather than GD, to find the optimum performance. In the vertical direction, the CD function is lesser than GD function. Furthermore, CD becomes broader once it is nearer the horizontal axis at the horizontal direction. Thus, the GD function has great probability to produce smaller perturbation, but not larger disturbance.

CD function has smaller perturbation capability than GD function, however, it is stronger than the GD in larger amount. It is predictable to have a high probability of moving away from a plateau or escaping from local optima, particularly if the "basin of attraction" of the plateau or local optima is larger compared to the size of the mean steep. Thus, the CD character function makes the algorithm the best global optimization and reliability and maintains population diversity. Therefore, the CD function gets the fittest solution. Hence, the CD is utilized in IWO technique rather than GD function. In general, weather conditions might change fast, thus, the study implemented MIWO approach.

In this work, $W_{\max}$ seeds are produced around the parent seed. Here, the same principle is used and produced $W_{\max}$ voltage point around the prior voltage value. Also, P&O algorithm is further added to produce the new voltage value. Therefore, newly evaluated PV power found from number might get from $W_{\max}$ number of voltages. Hence, the $W_{\max}$ amount of power points are evaluated for the enhanced $P_{pv}^{\max}$. This process is continued until the completion of search space. The new voltage value was attained using the following equations:

$$V_i^{j+1} = V_i^j + m\sigma_{iter} \times Cauchy(0,1) \times \left(V_{best} - V_i^j\right);\ i = 1,2,\dots,W_{max} \qquad (9)$$

In Eq. (9), V_{best} shows the best weed found in the entire population. V_i^j refers to the i^{th} weed location at j^{th} iteration. V_i^{j+1} denotes the update or new weed location at j^{th} iteration, δ_i stands for the standard CD random parameter.

$$m = \Delta V \times sign\left(\frac{dP_{PV}^{nrx}}{dV_{mpp}}\right) \qquad (10)$$

The fitness choice is a key factor in the MIWO method. An encoder outcome was applied for measuring the goodness of solution candidate. Here, the value of accuracy is the primary state exploited for designing a FF.

$$Fitness = \max(P) \qquad (11)$$

$$P = \frac{TP}{TP + FP} \qquad (12)$$

Where TP and FP depicts the true and false positive values.

IV. Results and Discussion

In this article, the DDoS attack recognition outputs of the MIWO-ELM approach is tested on the WSN-DS database, containing 5000 samples and 5 classes as represented in Table 1.

TABLE I. Dataset Details

Class	Total Samples
Normal	1000
Grayhole	1000
Blackhole	1000
Flooding	1000
Scheduling	1000
Total No. of Samples	5000

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8093
***Article Received:** 24 June 2023 **Revised:** 23 August 2023 **Accepted:** 06 September 2023*

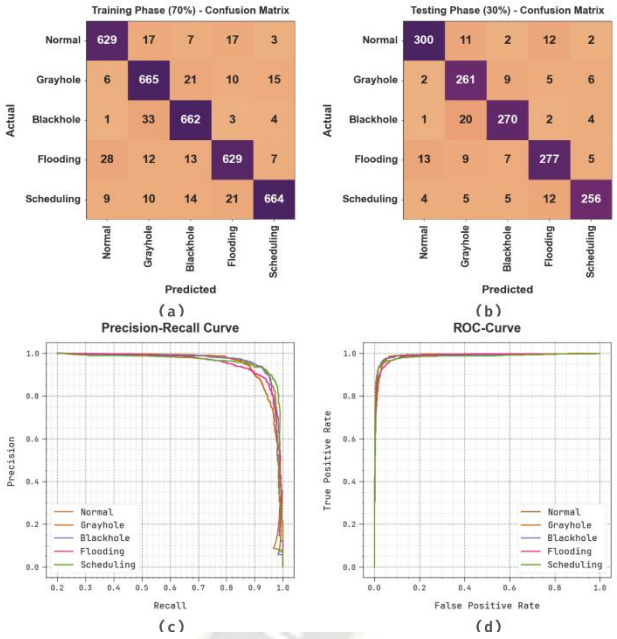

Figure 3. Classifier output of (a-b) Confusion matrices, (c-d) PR and ROC Curve

Fig. 3 establishes the classifier outcomes of the MIWO-ELM method on test dataset. Figs. 3a-3b represents the confusion matrix given by the MIWO-ELM method on 70:30 of TRP/TSP. The result stated that the MIWO-ELM approach has recognized and classified all 5 classes accurately. In addition, Fig. 3c reveals the PR curve of the MIWO-ELM approach. The outcome implied that the MIWO-ELM technique has accomplished greater PR achievement under 5 classes. At last, Fig. 3d exemplifies the ROC curve of the MIWO-ELM technique. The output described that the MIWO-ELM technique has produced capable outcome with higher ROC values under 5 classes.

In Table 2 and Fig. 4, the entire DDoS outbreak recognition outcomes of the MIWO-ELM approach is reported. The results stated that the MIWO-ELM approach recognizes all classes proficiently. With 70% of TRP, the MIWO-ELM approach gains average $accu_y$, $prec_n$, $sens_y$, $spec_y$, and F_{score} of 97.13%, 92.89%, 92.83%, 98.21%, and 92.84% respectively. Also, with 30% of TRP, the MIWO-ELM system gains average $accu_y$, $prec_n$, $sens_y$, $spec_y$, and F_{score} of 96.37%, 90.98%, 90.95%, 97.74%, and 90.93% correspondingly.

TABLE II. DDOS ATTACK RECOGNITION OUTCOME OF MIWO-ELM METHOD ON 70 AND 30 PERCENT OF TRP/TSP

Class	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$	F_{Score}
Training Phase (70%)					
Normal	97.49	93.46	93.46	98.44	93.46
Grayhole	96.46	90.23	92.75	97.41	91.47
Blackhole	97.26	92.33	94.17	98.03	93.24
Flooding	96.83	92.50	91.29	98.19	91.89
Scheduling	97.63	95.82	92.48	98.96	94.12
Average	**97.13**	**92.87**	**92.83**	**98.21**	**92.84**
Testing Phase (30%)					
Normal	96.87	93.75	91.74	98.29	92.74
Grayhole	95.53	85.29	92.23	96.30	88.62
Blackhole	96.67	92.15	90.91	98.09	91.53
Flooding	95.67	89.94	89.07	97.39	89.50
Scheduling	97.13	93.77	90.78	98.60	92.25
Average	**96.37**	**90.98**	**90.95**	**97.74**	**90.93**

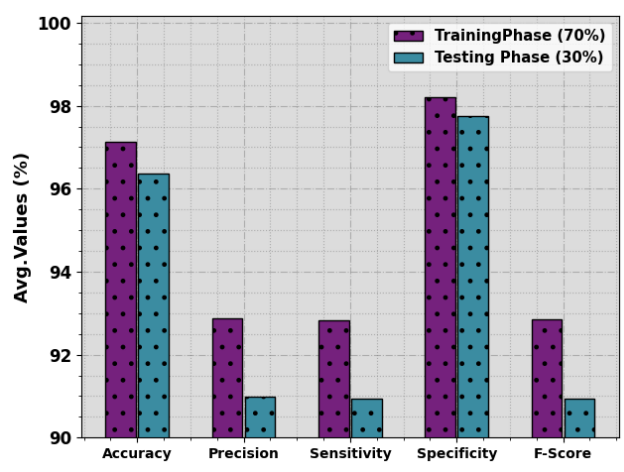

Figure 4. Average output of MIWO-ELM method on 70 and 30 percent of TRP/TSP

Figure 5. Accuracy curve of the MIWO-ELM method

Fig. 5 scrutinizes the MIWO-ELM system's accuracy during validation and training procedure on test data. The figure represented that the MIWO-ELM model reaches maximum value of accuracy over growing epochs. Furthermore, the maximum accuracy of validation over training accuracy exhibitions that the MIWO-ELM model will be learning effectively on test data.

The loss evaluation of the MIWO-ELM system during validation and training is exemplified on test data in Fig. 6. The output indicated that the MIWO-ELM technique attains close

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8093
***Article Received:** 24 June 2023 **Revised:** 23 August 2023 **Accepted:** 06 September 2023*

validation and training loss values. The MIWO-ELM technique learns capably on test data.

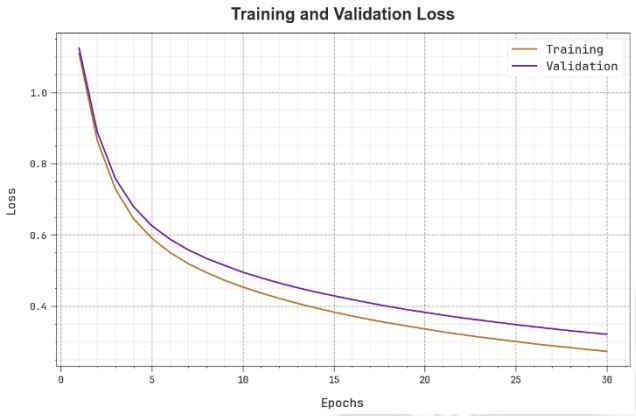

Figure 6. Loss curve of the MIWO-ELM system

TABLE III. TABLE 3. RELATIVE OUTPUT OF MIWO-ELM APPROACH WITH OTHER RECENT METHODS

Methodology	$Accu_y$	$Prec_n$	$Sens_y$	$Spec_y$
Bagging	93.50	89.61	91.97	97.18
Stacking	95.67	89.65	90.16	97.76
Boosting	95.07	91.21	90.19	95.36
WSS Algorithm	94.78	91.60	90.73	96.37
MIWO-ELM	97.13	92.87	92.83	98.21

Finally, a widespread comparison study of the MIWO-ELM approach with current approaches are exemplified in Table 3 and Fig. 7. The outputs portray that the MIWO-ELM approach resulted in improved results. Based on $accu_y$, the MIWO-ELM technique provides improving value of 97.13% while the bagging, stacking, boosting, and MIWO-ELM models attain decreasing values of 93.50%, 95.67%, 95.07%, and 94.78% respectively.

Meanwhile, with respect to $prec_n$, the MIWO-ELM method offers enhance value of 92.87% while the bagging, stacking, boosting, and MIWO-ELM models attain decreasing values of 89.61%, 89.65%, 91.21%, and 91.60% respectively. Moreover, based on $sens_y$, the MIWO-ELM approach offers improving value of 92.83% while the bagging, stacking, boosting, and MIWO-ELM models gain lesser values of 91.97%, 90.16%, 90.19%, and 90.73% respectively. Thus, the MIWO-ELM models can be implemented for precise DDoS recognition of outbreaks in WSN.

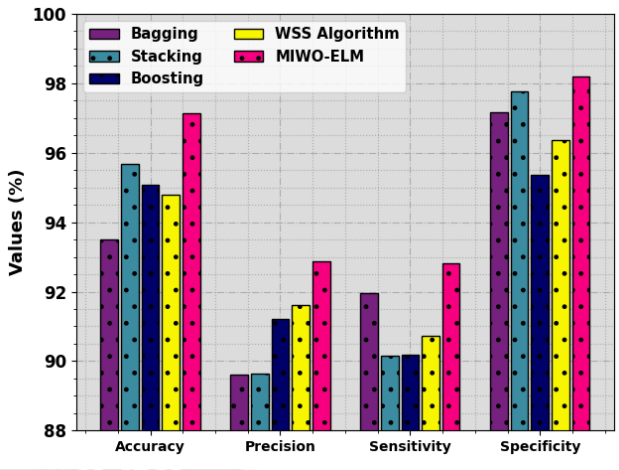

Figure 7. Relative output of MIWO-ELM approach with other recent techniques

V. CONCLUSION

In this research, a new MIWO-ELM model for accurate and automated recognition of DDoS outbreaks in the WSN environment. The presented MIWO-ELM model comprises three major processes such as data normalization, ELM based DDoS recognition of outbreak, and MIWO based tuning process. In the presented MIWO-ELM technique, an initial stage of data pre-processing is conducted. For accurate classification and recognition of DDoS outbreak process, the ELM technique can be applied. At last, the MIWO model can be exploited for the tuning process of the ELM model which leads to improved classification performance. The experimental analysis of the MIWO-ELM method takes place using WSN dataset. The comprehensive simulation outputs show the remarkable performance of the MIWO-ELM method compared to other recent approaches.

REFERENCES

[1] Salmi, S. and Oughdir, L., 2023. Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. Journal of Big Data, 10(1), pp.1-25.

[2] Mittal, M., Kumar, K. and Behal, S., 2022. Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Computing, pp.1-37.

[3] Sharma, H.S., Singh, M.M. and Sarkar, A., 2023, January. Machine Learning-Based DoS Attack Detection Techniques in Wireless Sensor Network: A Review. In Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021, Volume 2 (pp. 583-591). Singapore: Springer Nature Singapore.

[4] 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.

[5] Mihoub, A., Fredj, O.B., Cheikhrouhou, O., Derhab, A. and Krichen, M., 2022. Denial of service attack detection and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
DOI: https://doi.org/10.17762/ijritcc.v11i11s.8093
***Article Received:** 24 June 2023 **Revised:** 23 August 2023 **Accepted:** 06 September 2023*

mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering, 98, p.107716.

[6] Rao, G.S., Harshitha, M., Joshitha, V.R., Sravya, S.S. and Priya, M.V., 2023, March. DoS Attack Detection in Wireless Sensor Networks (WSN) Using Hybrid Machine Learning Model. In 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN) (pp. 384-388). IEEE.

[7] Ju-Hyuck, H. ., & Yong-Suk, K. . (2023). A Study on the Artificial Intelligence Model of White Blood Cell Counts Prediction Using Gan. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 165–173. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2584.

[8] Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E., Harold Robinson, Y. and Shanmuganathan, V., 2021. Machine learning based detection and a novel EC-BRTT algorithm based prevention of DoS attacks in wireless sensor networks. Wireless Personal Communications, pp.1-25.

[9] Quincozes, S.E. and Kazienko, J.F., 2020, June. Machine learning methods assessment for denial of service detection in wireless sensor networks. In 2020 IEEE 6th World Forum on Internet of Things (WF-IoT) (pp. 1-6). IEEE.

[10] 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.

[11] Sherazi, H.H.R., Iqbal, R., Ahmad, F., Khan, Z.A. and Chaudary, M.H., 2019. DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. Sustainable Computing: Informatics and Systems, 23, pp.13-20.

[12] Pise, D. P. . (2021). Bot Net Detection for Social Media Using Segmentation with Classification Using Deep Learning Architecture. Research Journal of Computer Systems and Engineering, 2(1), 11:15. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/13

[13] GSR, E.S., Ganeshan, R., Jingle, I.D.J. and Ananth, J.P., 2023. FACVO-DNFN: Deep learning-based feature fusion and Distributed Denial of Service attack detection in cloud computing. Knowledge-Based Systems, 261, p.110132.

[14] Kadam, N. and Krovi, R.S., 2021. Machine learning approach of hybrid KSVN algorithm to detect DDoS attack in VANET. International Journal of Advanced Computer Science and Applications, 12(7).

[15] Al-Hadhrami, Y. and Hussain, F.K., 2020. A machine learning architecture towards detecting denial of service Attack in IoT. In Complex, Intelligent, and Software Intensive Systems: Proceedings of the 13th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS-2019) (pp. 417-429). Springer International Publishing.

[16] Muhammad Rahman, Automated Machine Learning for Model Selection and Hyperparameter Optimization , Machine Learning Applications Conference Proceedings, Vol 2 2022.

[17] 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.

[18] Mhamdi, L., McLernon, D., El-Moussa, F., Zaidi, S.A.R., Ghogho, M. and Tang, T., 2020, October. A deep learning approach combining autoencoder with one-class SVM for DDoS attack detection in SDNs. In 2020 IEEE Eighth International Conference on Communications and Networking (ComNet) (pp. 1-6). IEEE.

[19] Sait, A.R.W., Pustokhina, I. and Ilayaraja, M., 2021. Mitigating DDoS attacks in wireless sensor networks using heuristic feature selection with deep learning model. Journal of Cybersecurity and Information Management, (2), pp.65-5.

[20] Zhou, B., Li, J., Wu, J., Guo, S., Gu, Y. and Li, Z., 2018, May. Machine-learning-based online distributed denial-of-service attack detection using spark streaming. In 2018 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[21] Iqbal, N., Jamil, F., Ahmad, S. and Kim, D., 2021. A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services. IEEE Access, 9, pp.8069-8098.

[22] Prof. Prachiti Deshpande. (2016). Performance Analysis of RPL Routing Protocol for WBANs. International Journal of New Practices in Management and Engineering, 5(01), 14 - 21. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/43.

[23] Chen, Z., Yang, J., Feng, Z. and Chen, L., 2022. RSCNet: An Efficient Remote Sensing Scene Classification Model Based on Lightweight Convolution Neural Networks. Electronics, 11(22), p.3727.

[24] Senapati, M.K., Pradhan, C. and Calay, R.K., 2023. A computational intelligence based maximum power point tracking for photovoltaic power generation system with small-signal analysis. Optimal Control Applications and Methods, 44(2), pp.617-636.