International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

WSN Attack Detection Using Attentive Dual Residual Generative Adversarial Networks

Sivanesan N.[1*], Rajesh A.[2], K. S. Archana[3]

Submitted: 10/05/2023 **Revised**: 15/07/2023 **Accepted**: 05/08/2023

Abstract: Wireless sensor networks (WSN) play an important role in different industries because of lack infrastructure but remain vulnerable to numerous attacks. Denial-of-Service (Dos) attacks are the main attack that scares WSN. If a DoS attacks targets a company, it could lower that company's perceived value in the market. To minimize these issues this research article presents an approach of a WSN Attack detection using Attentive Dual Residual Generative Adversarial Networks (WSN-AD-ADRGAN) technique. Initially, input data is collected from WSN-DS. Afterward the data are fed to preprocessing. The pre processing segment removes noise and redundant data by utilizing Adaptive distorted Gaussian matched filter (ADGMF)and the preprocessed output fed to Attentive Dual Residual Generative Adversarial Networks (ADRGAN) method that classifies the WSN attacks into Black hole attack, Grey hole attack, Flooding attack, Timing attack ,normal. Attentive Dual Residual Generative Adversarial Network classifier, in general, does not describe modifying optimization techniques to identify optimum parameters to enable accurate WSN attack classification. Therefore, it is proposed to use Ladybug Beetle Optimization Algorithm (LBOA) to optimize Attentive Dual Residual Generative Adversarial Network, which accurately classifies WSN attacks. The proposed WSN-AD-ADRGAN technique is implemented in python utilizing WSN-DS dataset. The suggested method's performance is examined using performance metrics like precision, recall, accuracy, F1-score, specificity, ROC, computing time. The proposed AIPE-DBO-LDC-CXR method attains higher accuracy 16.65%, 18.85% and 16.45%; greater sensitivity 16.34%, 12.23%, and 19.12%; greater specificity 14.89%, 16.89% and 20.67% and 82.37%, 87.76% and 78.78% lower computational time analyzed to the existing methods like intrusion identification system in WSN utilizing conditional generative adversarial network (IDS-WSN-CGAN),Service attack improvement in wireless sensor network under machine learning (SAI-WSN-ML),Machine learning based identification, EC-BRTT technique based DoS attacks prevention in wireless sensor networks (ML-DDoS-WSN) respectively.

***Keywords*:** *Adaptive distorted Gaussian matched filter, Attentive Dual Residual Generative Adversarial Networks, Ladybug Beetle Optimization, Wireless Sensor Network.*

1. Introduction

In Wireless network contains a wide range of applications, including communication, internet services, and indoor and outdoor monitoring applications. These established networks are used to transport a data variety. [1-3]. Considering the wide range of attacks and security breaches that might occur in the modern world, there is an urgent need for security enhancements for these different networks. We also require appropriate network protection techniques given that steadily growing amount of data being transmitted across various entities and networks. The WSNs are used for many kinds of objectives including data aggregation, information sensing, environment monitoring, digital agriculture, smart agriculture, remote sensing, health care, armed missions, border surveillance [4]. Among two nations line of control, when troops and Soldiers are deployed to police these locations; it is not always possible to monitor people.

WSN is a free Wi-Fi network set up ad hoc using huge count of Wi-Fi sensors to reveal the social, physical, environmental conditions. These sensors are linked with the bottom Station that serves as WSN machine's processing unit. In the context of WSN, aspects like energy consumption reduction and sensor network security is the subject of numerous articles [5]. Additionally, excessive network activity indicates security problem avoided during the routing process to prevent sudden resource shortages. The lifetime of the network is the time required for all sensors to provide coverage. Enhancing the network's lifetime is important because the sensor nodes are typically restricted battery-powered, and WSN suffers from a number of significant restrictions like inadequate memory, limited computing capability, and limited and non-rechargeable battery power [6].

The key contributions of this paper includes;

- In this manuscript, the WSN attacks detection using WSN-AD-ADRGAN is proposed.

[1*]*Research Scholar, Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advance Studies (VISTAS), Chennai, India*
[1*]*Email: profnsivanesan@gmail.com*
[2]*Professor, Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advance Studies (VISTAS), Chennai, India*
[2]*Email: arajesh.se@velsuniv.ac.in*
[3]*Assistant Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattakulathur, Chengalpattu, District- 603203, India.*
[3]*Email: archanak1@srmist.edu.in*
[*]*Corresponding author Email: profnsivanesan@gmail.com*

- To find WSN attack that can be used to evaluate WSN attack detection using Adaptive distorted Gaussian matched filter (ADGMF) [15]technique, and to propose a detection model of classification using Attentive Dual Residual Generative Adversarial Networks (ADRGAN) [16], optimized Ladybug Beetle Optimization (LBO) [17].
- A variety of ADRGAN is evaluated to calculate the values for various parameters such as accuracy and ROC. This is done in order to find the most effective model for detecting the classification.
- Performance of the proposed methodology WSN-AD-ADRGAN has been evaluated and compared with the existing IDS-WSN-CGAN, SAI-WSN-ML and ML-DDoS-WSN methods respectively.

The remaining manuscripts are structured as follows: part 2 analyzes Literature survey, part 3 defines proposed approach; part 4 illustrates results; and part 5 presents conclusion.

2. Literature Survey

Numerous research works presented in the literature to classify WSN attack detection using deep learning; a few current works are described below.

Sood et al., [7] presented an intrusion detection system in WSN utilizing CGAN. Present an IDS model that makes use of the CGAN, enables unsupervised learning and provides extreme learning component. Using the gradient boosting (XGBoost) classifier to compare and view results more quickly. With the help of a multi-layer network, the technique learns from samples in dataset for an improved training procedure. The dataset is collected from NSL-KDD and CICIDS2017 used as a detector for cyber intrusions. It provides high accuracy with low computation time.

Yu et al., [8] presented Service attack enhancement in WSN depending on machine learning. Security was increased by identifying attackers through denial-of-service attacks and responding to WSN. These two machine learning methods, media access control (MAC) layer assaults detection and support vector machine (SVM) detection use neural networks (NN) and SVM, respectively. It has a MAC wireless sensor node with an access channel. A protective covering is necessary. Use WSN for scenario likelihood. Vanderbilt's plough error simulation and wireless network simulator. It provides better accuracy and it was more expensive.

Lakshmi Narayanan et al., [9] presented Machine learning based identification and EC-BRTT technique based DoS attacks prevention in WSN. In the presented paper, two crucial attacks provided that includes Machine Learning basis Naive Bayes Classifier, Enhanced Code basis Round Trip Time-based approach. The presented model validated on network simulator. The presented method utilized to reduce the communication overhead. It provides high precision with low accuracy.

Kavousi-Fard et al., [10] presented machine learning based cyber-attack detection method for WSN in micro grids. The precise protected structure to identify and prevent data integrity risks is provided in WSN in micro grids. To identify malicious attacks of various intensities during a secured operation, a method for intelligent anomaly detection based on prediction intervals was presented. In order to offer the best possible PIs over the readings from smart meters at electric consumers; it attains high f1-score with low specificity

Rabi et al., [11] presented IoT routing attacks detection utilizing machine learning methods. The presented paper focus on WSN that represents The Internet of Things' basic blocks, Routing Protocol for Low power and Lossy Network, are vulnerable to routing assaults. Additionally, we outline some ideas for ongoing research on intrusion detection and create a method for identifying three different RPL sort assaults. The simulation was done utilizing Contiki-Cooja four network scenarios like one malicious, three normal, presenting different attacks. It provides high sensitivity with low f1-score.

Kurtkoti et al., [12] presented the effectiveness of machine learning techniques for recognizing and reducing black as well as gray-hole assaults. The presented paper followed a study of various machine learning (ML) algorithms in identifying these attacks; a proposal for mitigating such attacks is made. By using a malicious node to simulate grey hole and black hole attacks, the WSN-DS dataset obtained. The classification models using the presented dataset include nine alternative ratios for training and testing. For each attacks, performance indicators including accuracy and execution time for different classifiers were examined. It attains high computational time with low precision.

Elsadig [13] presented Detection of Denial-of-Service Attack in Wireless Sensor Networks: A lightweight Machine Learning Method, focus on DoS attacks, this study clarifies the limitations, vulnerabilities, and security risks associated with WSNs. The effectiveness and shortcomings of recent approaches for DoS attack detection examined to identify DoS attacks in WSNs, the presented work presented minimal machine learning identification strategy depend on the decision tree technique and Gini feature selection method. The presented method was trained and verified utilizing an improved WSN-DS dataset. It provides high precision but durability was decreased.

3. Proposed Methodology

In this section, WSN Attack identification utilizing WSN-AD-ADRGAN discussed. The block diagram of the proposed WSN-AD-ADRGAN attack classification is presented in Figure 2. Dataset, Pre-processing, Classification, and Optimization are the four processes that make up this procedure. Consequently, a full explanation of each stage is provided below,

3.1 Dataset

The proposed WSN attack detection method is trained and assessed the dataset. The dataset is collected from WSN-DS dataset [14] for detecting and evaluating model with the performance metrics. The most important data processing methods, as deep learning algorithms assist in the generation of reliable data. There are numerous algorithms available, and the model is selected based on the issue. The dataset contains four types of attacks include black hole, gray hole, flooding, timing. The data modeling is given in Figure 1;

Fig 1: Data modeling process

3.2 Preprocessing using Adaptive distorted Gaussian matched filter

In this step ADGMF performs the data preprocessing. Deep learning models cannot directly use data that is noisy, unimportant, or of the inefficient type. Cleaning up data and preparing it for deep learning models is a process that must be done during data preprocessing. The residual model is described by the equation (1)

$$H(s,\{U_i\}) = F(s) - s \tag{1}$$

let s denotes input feature map, $\{U_i\}$ represents i^{th} layer weight and $F(s)$ denotes desired mapping to learn. To learn the identity function and it is defined by the equation (2)

$$F(s) = H(s,\{U_i\}) + s \tag{2}$$

Let, s implies input feature map, $\{U_i\}$ represents i^{th} layer weight, $F(s)$ denotes desired mapping to learn. Equation (2) attains through short cut connections that connect block's input feature map including output, allowing for the addition of both utilizing this structure by residual architecture with ADGMF. The filters output is computed is defined by the equation (3)

$$W_j(s,r) = \max\{K_j^{(\theta)}(s,r)\} \tag{3}$$

here (s,r) denotes input feature map domain position , $\{W_j\}$ represents filter output sets in layer; The final modified or replaced filter will removed the noise in the input data these preprocessing data is fed into classification figure 2.

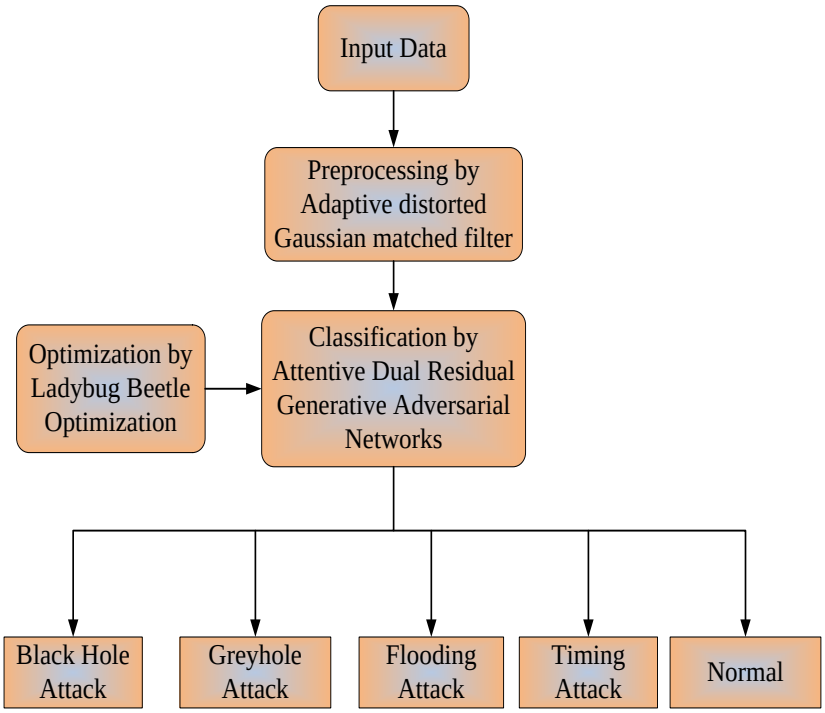

Fig 2: Block diagram for the proposed WSN-AD-ADRGAN methodology

3.3 Classification using Attentive Dual Residual Generative Adversarial Networks

This section discusses the ADRGAN. Utilizing adversarial training the general application of GAN generate results from game theory to deep learning neural networks that are precise and lifelike.

So, employing GAN can create a rain-like layer removal network that essentially has three components: a generator, a guide, and a discriminator. The function of GAN is defined by the equation (4)

$$R(V,S)=\mathrm{E}_{D\sim T_{clean}}[\log(S(D))]+\mathrm{E}_{L\sim T_{rain-like\,layer}}[\log(1-S(V(L))] \quad (4)$$

here V and S refers to discriminator and generator. L, denotes the generator input and sample with rain-like layer. D, refers clean images; Mask pictures are generated using a threshold-based binary categorization algorithm defined by the equation (5)

$$Loss\_Total=\frac{1}{2}*Loss\_Mask+\frac{1}{2}*Loss\_Overall \quad (5)$$

here $Loss\_Mask$ represents rain-like layer loss value and $Loss\_Overall$ indicates whole value loss value image. The error produced by adding the complete differences among the goal value and estimated value is loss function. It is defined by the equation (6)

$$L1(x,x)=\sum_{j=0}^{n}\left|x^{(j)}-x^{(j)}\right| \quad (6)$$

here $x^{(j)}$ denotes the value of every pixel on the target image, and $x^{(j)}$ represents estimation image. The resultant data was then categorized as the attacks of Black hole, Grey hole, Flooding, Timing, Normal. Because of its convenience, pertinence, the artificial intelligence-based optimization strategy is taken into account in the ADRGAN classifier. In this work, LBO is employed to optimize the ADRGAN optimum parameter R. Here, LBO is employed for tuning the weight and bias parameter of ADRGAN.

3.3.1 Stepwise procedure for Lady bug Beetle Optimization

Here, the stepwise process is described to obtain ideal values of ADRGAN using LBO. This technique involves evaluating and sorting the original population of algorithms according to their evaluation. The population is then revised and updated. The most effective choice is reported following sufficient updates and evaluations for the population. The synchronized movements of ladybirds in search of the best spot in nature act as an inspiration for LBO. The comprehensive step's method is then described as follows:

Step1: Initialization

Initialize the population of Ladybug Beetle optimizing the weight parameter values of generator R from Attentive Dual Residual Generative Adversarial Networks. It is defined by the equation (7)

$$Q_i = \frac{f(y_i(t))}{\sum_{k=1}^{M^t} f(y_k(t))} \quad (7)$$

here Q_i equals ratio of i^{th} proportion of every ladybird's cost to all ladybirds' combined costs in the t^{th} iteration of the suggested optimization process.

Step 2: Random Generation

Where the random number falls within the division is established. It is obvious that the ladybird with the warmer environment has an increased chance of choosing. Thus it is defined by the equation (8)

$$D_i = e^{-\beta \frac{h(y_r(t))}{h_{worst}}} \quad (8)$$

here β denotes pressure co-efficient in the Roulette-wheel selection method and h_{worst} represents objective function's worst value up until the current generation.

Step 3: Fitness function

From the initialized assessments, the outcome is the random answer. The evaluation of the fitness function uses the results of weight parameter optimization R . Thus, it is defined by the equation (9),

$$fitness\ function = Optimizing\ [R] \quad (9)$$

Step 4: Exploration Phase

Exploring frontiers in the search space and avoiding the local minima require considering account of the mutation in the population updating process. The number of i^{th} ladybug's decision factors altered and it is defined by the equation (10)

$$m_n = round(m * \mu_n) \quad (10)$$

here μ_n denotes mutation rate m represents the decision variable length. The m_n variables of the i^{th} ladybug's available m variables are chosen at random. Then, the chosen position of the i^{th} ladybird is substituted for the random variables in the viable region.

Step 5: Exploitation phase for optimizing R

Exploitation is the final stage, during which a security tester actively takes advantage of security flaws in the system under evaluation. LBOs exploitation phase is defined by the equation (11)

$$M(t+1) = round\left(M(t) - rand \times M(t)\left(\frac{NFE}{NFE_{\max}} \right) \right) \quad (11)$$

here NFE represents the number of function evaluations, $NFE_{\max}$ indicates the maximum of NFE . Thus the exploitation is defined.

Step 6: Termination

In this step, the weight parameter is R , from Attentive Dual Residual Generative Adversarial Networks are optimized with the help of LBO, will repeat the functions until the position information $M_j = M + 1$ is met. Then finally WSN-AD-ADRDAN identifies the WSN attack with greater accuracy by decrease the computational time with error.

4. Result and Discussion

The experimental outcomes of proposed method are discussed in this segment. Then, the proposed method is simulated in Python under mentioned performance metrics. The obtained results of the proposed WSN Attack detection using WSN-AD-ADRGAN method analyzed with the existing IDS-WSN-CGAN [7],SAI-WSN-ML [8], ML-D DoS-WSN [9]methods respectively.

4.1 Performance measures

This is the important step for choosing optimal classifier. Performance measures are assessed to assess performance, including accuracy, ROC.

4.1.1 Accuracy

Accuracy measures the proportion of samples (positives and negatives) besides total samples and it is given by the eqn (12),

$$accuracy = \frac{TP + TN}{TP + TN + FN + FP} \quad (12)$$

4.1.2 ROC

It is the ratio of false negative to true positive area and it is computed by the equation (13)

$$ROC = 0.5 \times \left(\frac{TP}{TP + FN} + \frac{TN}{TN + FP} \right) \quad (13)$$

4.2 Performance Analysis

Figure 3-4 depicts the simulation outcomes of proposed WSN-AD-ADRGAN method. Then, the suggested WSN-AD-ADRGAN method is likened with existing IDS-WSN-CGAN, SAI-WSN-ML and ML-DDoS-WSN methods respectively.

Figure 3 depicts Accuracy analysis. The classification method's overall accuracy is up to 98%, making it a more accurate WSN attacks classification technique. Here, the proposed WSN-AD-ADRGN method attains 40.56%,

20.76%, and 20.67% higher Accuracy for Black hole attack, 35.50%, 23.65%, and 20.64% greater accuracy for Grey hole attack, 45.65%, 32.54% and 22.76% higher accuracy for Flooding attack, 40.35%, 20.87% and 21.43% greater accuracy for Timing attack, 35.76%, 30.23% ,20.27% greater accuracy for Normal, when evaluated to the existing IDS-WSN-CGAN, SAI-WSN-ML and ML-DDoS-WSN methods.

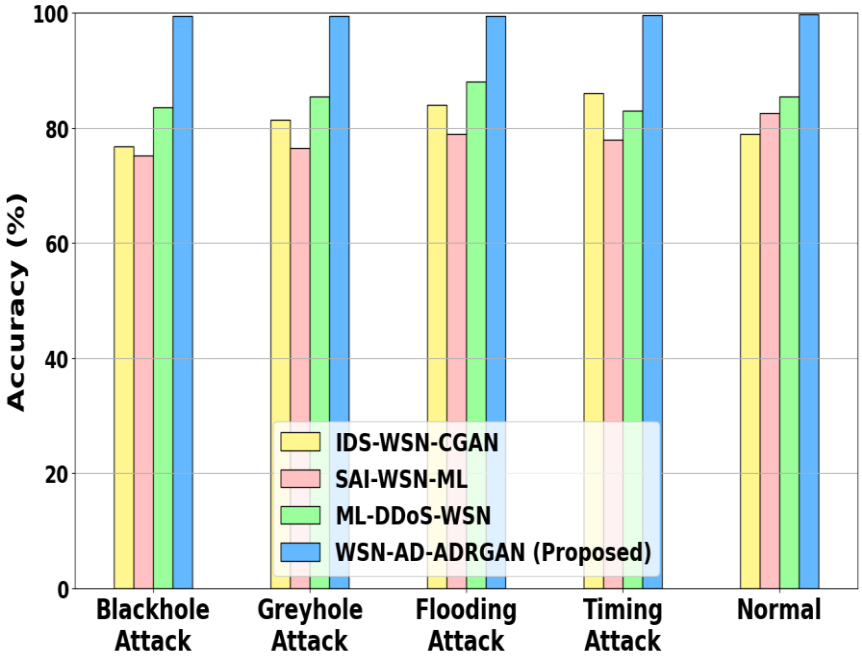

Fig 3: Accuracy Analysis

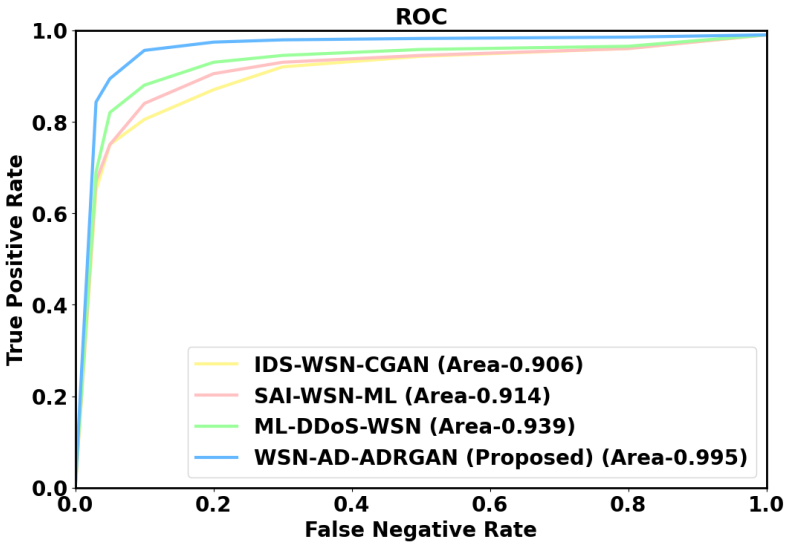

Fig 4: ROC Analysis

Figure 4 depicts the analysis of RoC. The proposed WSN-AD-ADRGAN technique then provides a greater ROC in 3.49%, 6.45% and 6.78% than the existing approaches which include IDS-WSN-CGAN, SAI-WSN-ML and ML-D DoS-WSN methods.

5. Conclusion

In this section, WSN attack detection using WSN-AD-ADRGAN. The proposed WSN-AD-ADRGAN approach is implemented in Python using WSN-DS dataset. The proposed WSN-AD-ADRGAN approach achieves greater F1-score 16.65%, 18.85% and 16.45%; greater specificity 16.34%, 12.23%, and 19.12%; greater sensitivity 14.89%, 16.89% and 20.67% and 82.37%, 87.76% and 78.78% lower computational time analyzed to the existing IDS-WSN-CGAN, SAI-WSN-ML and ML-DDoS-WSN methods.

Reference

[1] K. Cheena, T. Amgoth, and G. Shankar, 2023. Deep Learning-Based Black Hole Detection Model for WSN in Smart Grid. In *Computational Intelligence:*

Select Proceedings of InCITe 2022 (pp. 19-30). Singapore: Springer Nature Singapore.

[2] S. Karthic, and SM. Kumar, 2023. Hybrid optimized deep neural network with enhanced conditional random field based intrusion detection on wireless sensor network. *Neural Processing Letters*, *55*(1), pp.459-479.

[3] SE. Quincozes, JF. Kazienko, and VE. Quincozes, 2023. An extended evaluation on machine learning techniques for Denial-of-Service detection in Wireless Sensor Networks. *Internet of Things*, *22*, p.100684.

[4] S. Rajasoundaran, AV. Prabu, S. Routray, PP. Malla, GS. Kumar, A. Mukherjee. and Y. Qi, 2022. Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks. *Computer Communications*, *187*, pp.71-82.

[5] M. Dener, C. Okur, S. Al. and A. Orman, 2023. WSN-BFSF: A New Dataset for Attacks Detection in Wireless Sensor Networks. *IEEE Internet of Things Journal*.

[6] NM. Saravana Kumar, E. Suryaprabha, K. Hariprasath. and V. Vijayakumar, 2023. Deep Learning Based Hybrid Security Model in Wireless Sensor Network. *Wireless Personal Communications*, *129*(3), pp.1789-1805.

[7] T. Sood, S. Prakash, S. Sharma, A. Singh, and H. Choubey, 2022. Intrusion detection system in wireless sensor network using conditional generative adversarial network. *Wireless Personal Communications*, *126*(1), pp.911-931.

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

[9] K. Lakshmi Narayanan, R. Santhana Krishnan, E. Golden Julie, Y. Harold Robinson, and V. Shanmuganathan, 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.

[10] A. Kavousi-Fard, W. Su and T. Jin, 2020. A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids. *IEEE Transactions on Industrial Informatics*, *17*(1), pp.650-658.

[11] S. Rabhi, T. Abbes, and F. Zarai, 2023. IoT routing attacks detection using machine learning algorithms. *Wireless Personal Communications*, *128*(3), pp.1839-1857.

[12] M. Kurtkoti, BS. Premananda, and K. Vishwavardhan Reddy, 2022. Performance analysis of machine learning algorithms in detecting and mitigating black and gray hole attacks. In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021* (pp. 945-961). Singapore: Springer Nature Singapore.

[13] MA. Elsadig, 2023. Detection of Denial-of-Service Attack in Wireless Sensor Networks: A lightweight Machine Learning Approach. *IEEE Access*.

[14] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds

[15] DE. Alvarado-Carrillo, E. Ovalle-Magallanes, and OS. Dalmau-Cedeño, 2021. D-GaussianNet: Adaptive distorted Gaussian matched filter with convolutional neural network for retinal vessel segmentation. *Geometry and Vision* (pp. 378-392). Cham: Springer International Publishing.

[16] Q. Luo, H. He, K. Liu, C. Yang, O. Silven, and L. Liu, 2023. Rain-like Layer Removal from Hot-Rolled Steel Strip Based on Attentive Dual Residual Generative Adversarial Network. *IEEE Transactions on Instrumentation and Measurement*.

[17] S. Safiri, and A. Nikoofard, 2023. Ladybug Beetle Optimization algorithm: application for real-world problems. The Journal of Supercomputing, 79(3), pp.3511-3560.

[18] Dhabliya, D., Sharma, R. Cloud computing based mobile devices for distributed computing (2019) International Journal of Control and Automation, 12 (6 Special Issue), pp. 1-4.

[19] Dr. Antino Marelino. (2014). Customer Satisfaction Analysis based on Customer Relationship Management. International Journal of New Practices in Management and Engineering, 3(01), 07 - 12. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/26

[20] Ghazaly, N. M. . (2020). Secure Internet of Things Environment Based Blockchain Analysis. Research Journal of Computer Systems and Engineering, 1(2), 26:30. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/8