ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 10, Issue 9, September 2023

Machine Learning Algorithms for Detecting DDoS Attacks in Wireless Sensor Networks: A Conceptual Overview

[1] Jyothsna. B, [2] Dr. V. Jyothsna

[1] Research Scholar, Department of Information Technology, Mohan Babu University, Sree Sainath Nagar, Tirupati, Andhra Pradesh, India
[2] Associate Dean (Academics Affairs) and Associate Professor, Department of Information Technology, Mohan Babu University, Sree Sainath Nagar, Tirupati, Andhra Pradesh, India
Corresponding Author Email: [1] 22202R010017@mbu.asia

Abstract*— Wireless Sensor Networks are one of the base platform networks highly demanded by various real time applications recently. WSN has gained more attraction for various applications following the advancements of sensor devices and technologies. Agriculture, surveillance monitoring systems, healthcare monitoring, and smart environment are some of the applications fast-growing applications nowadays. Security is one of the major issues that remain in WSNs. Different kinds of malicious attacks are created dynamically anywhere in the WSN at any time. In any network, malicious activities destroy the data transmission process and compromise the other legitimate nodes. Several earlier pieces of research stated that WSN meets security issues because of its restricted infrastructure and physical security. Any sensor can communicate with other sensors, creating an opportunity for various vulnerable attacks affecting legitimate network nodes. Since nodes are tiny, inexpensive, and easy to deploy anywhere without any constraints identifying malicious nodes during the deployment stages is impossible. Various earlier research works have proposed security mechanisms that could not effectively detect malicious threats and attacks. The detailed literature of several proposed methods using machine learning algorithms in the past 10 years is explained here. It is also presented a comparative analysis of different machine learning algorithms used for DoS attack detection in WSN with simulation results. The accuracy comparison is given, and it shows that the SVM model outperforms Random Forest, Logistic Regression, and Decision trees.

Keywords: DoS Attack, WSN, Machine Learning Algorithm, Malicious Node Detection, WSN Security.

I. INTRODUCTION

Denial of service (Dos) is a threat that makes it difficult or impossible for the users to access the application or network or sometimes shut down a network. Dos attains this by flooding prey with the traffic or sending particular that setoff crash. Restarting the system solves the problem instantly; however, flooding attacks are more vulnerable and difficult to recover from. Intruders of these types usually flood wireless sensor networks with traffic staggering the victim network, making it hard to access them. Some examples of the Dos attack are Black Friday sales, where intruders run fake campaigns using untrustworthy websites during Black Friday. The standard Dos attack tools include tools for IP address spoofing and ping of death (an attack where the intruders target the victim with oversized packet data), resulting in crashes, freezes, and destabilization of computers or networks. This type of DOS targets and exploits the weakness the establishment have been patched.

Dos attack started in 1988 with the Robert Morris worm attack has a long history where a worm was detected and quickly spread through the network and triggered a DoS attack on the victim system. Dos attack targets more than one of the layers in the OSI model layer; the most vulnerable layers prone to attack are the network, transport, presentation, and application layers. Using user datagram protocol (UDP) is one common way of attacking the OSI layer model, sending packets before the receiving data packets send the packet for agreement. Another common attack is a synchronization packet attack, where packets are sent to all open ports on a server using a fake IP address or spoofed one. These attacks are hard to identify in the network. Signs of a DoS attack are more email, inability to access the website, or degraded network performance.

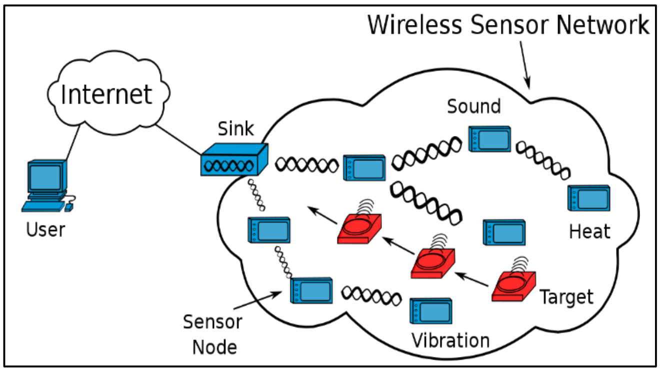

Figure-1. General Structure of WSN

Figure-1 shows the structure of a WSN. The structure of WSN consists of different topologies for radio communication. Wireless sensor networks are a network used in industrial applications such as industrial process monitoring and control machines WSN is built of nodes that connect with another sensor, and WSN is a system designed to monitor remotely. WSN is widely used in agriculture, whereas it is an infrastructure-less network to monitor environmental conditions such as sound, vibration, and pressure WSNs have limited processing speed, communication bandwidth, and storage capacity. One of the limitations of WSN is that it is wireless, it is prone to hackers, and it is designed for low-speed applications; hence it is not suitable for high-speed communication; it is a dynamic network topology where the unused nodes have been disabled to adapt their topology by the network. Limitations of WSN are the heterogeneity of nodes where nodes differ from each other, where cluster-based routing protocols are proposed to handle heterogeneity in WSN. One of the common names with limited sensor nodes and power are vulnerable to many kinds of wireless attack sensor network is one with limited resources and power.

This paper contributes a detailed survey discussion about decision trees, random forests, and support vector machines for detecting DoS attacks. The machine learning algorithms are explained pictorially with mathematical equations. It also presents the simulation output in terms of accuracy.

II. LITERATURE REVIEW

This section reviews and discusses various existing research works to find the optimal solutions to avoid threats in a wireless sensor network. Primarily this research work has mainly focused on projecting the efficiency of machine learning and deep learning-based detection technique to secure the WSN system from the DOS attack. Baig et al. (2006) said that unauthorized functions in WSNs make the network riskier. So, attackers can easily hack the model and inject the DoS type of attack. DoS is one of the major threats, and it is more harmful due to its imperative nature. You and Tsai (2008) have discussed the efficiency and features of WSNs. WSN is a decentralized controlling system connected through various wireless sensor devices and radio links. It effectively creates communication between the nodes in the network. The author Das et al. (2010) define that AI-based technique provides various features to the WSN-based system. It comprises two different learning algorithms such as machine and deep learning. The AI-based techniques have improved the WSN system's quality in detecting intrusion in the network model. It includes various biological features for producing the result, such as NN, evolutionary algorithm, and fuzzy systems. Pelechrinis et al. (2011) have stated that security is one of the major concerns in all communication networks. In that sense, in WSN also, security is considered an important part. In order to improve the efficiency of the proposed model, various security systems are implemented. Pelechrinis et al. (2011) have stated that security is one of the major concerns in all communication networks. In that sense, in WSN also, security is considered an important part.

In order to improve the efficiency of the proposed model, various security systems are implemented. Alsheikh et al. (2014) define the WSN network as a more suitable tool for communicating the various nodes in the network. A base station is a component used to connect or create a link between the nodes. Chang et al. (2016) and Ogbodo et al. (2017) said that WSN, distributed communication systems, and accurately sensing the data through sensors are one of the main features of WSN. It is used in many real-time applications such as healthcare, school, industries, business sectors, and data centers. The following authors ((Di and Er (2007), Shiaeles et al. (2012), Patil and Gaikwad (2015), Mallikarjunan. (2016), Mazur et al. (2016), M.A. Rahman et al. (2017); and Gavrić and Simić, (2018)) from various articles stated that Injecting the DoS into the WSN is not easier to perform—DoS attack function by executing the attack into the main server of the wired and wireless system. Once the system attacked, the DoS attacks multiplied and damaged the other network files. So a new advanced technique is required to overcome the issues in WSN. For that, various learning algorithms have been proposed by various authors. Gunduz et al. (2015) define various machine algorithms to accurately identify the optimal model to detect intrusion from the input datasets. The authors have examined the efficiency of the proposed model by performing various simulation tasks. The result of the model indicates that the ML-based model effectively detects intrusion in the input datasets.

Lokas et al. (2017) developed an LSTM-based model to detect cyber-attacks in WSNs. It is specially developed to detect DoS attacks from the input data. The experimental result shows that the proposed LSTM-based model detects the threats with 86.9% accuracy. When compared to other methods, the proposed model performs better. The SVM model performs better with 96.7% accuracy compared to other methods. Abdullah et al. (2018) proposed various ML classifiers, such as SVM, NB, RF, and DT, to detect intrusion in WSNs. To train and classify the proposed model WSN-DS datasets and WEKA tool, respectively. Park et al. (2018) suggested an RF model detect the DoS attack in WSN-DS datasets. The proposed model has effectively detected the black hole, grey hole, TDMA, flooding, and Normal attack with 99%, 98%, 96%, 96%, and 100% F1-score values with 97.8% accuracy. Almomani et al. (2018) suggested various ML algorithms such as NB, RF, DT, SVM, KNN, BN, ANN, and J48 to detect DoS attacks in WSNs. Based on the previous survey work, the feature selection process is performed. The result of the analysis emphasizes that the RF model performs better than the other by achieving a 99.7% accuracy result. Followed by this, ANN has achieved the final classification result with a 98.3% true positive value. Lee et al. (2018) proposed three classification algorithms: DNN, RNN, and Self-taught learning (STL). The efficiency of the proposed model is evaluated using various performance metrics such as precision, recall, F1-score, and accuracy. The evaluation results show that the STL and LSTM models classify the attacks with 98.9% and 79.20% accuracy, respectively.

Y. Shen et al. (2018) have proposed a new method called Bat Algorithm to detect intrusion detection (IDS). Base Classifier is an Extreme Machine Learning (ELM) method that uses three public datasets, namely KDD99, NSL, and Kyoto. The proposed system gives a good performance. Based on the performance of the ensemble method, it will reduce the substantial computing resources. GPU (graphics processing unit) is implemented and evaluated by the KDD Cup '99 and NSL-KDD datasets. N. Shone et al. (2018) introduced a DL intrusion detection method. They have also used the NDAE system to extract the feature learning process and classification method. Compared with the other methods, it gives a good performance. M.H Ali et al. (2018) have utilized the FLN-based PSO (Fast Learning Network-based particle swarm optimization). This model is used to detect the problem in intrusion detection, and KDD99 is validated from the famous dataset. Various optimization techniques are used, but the proposed work outperformed well. B. Yan and G. Han (2018) have suggested a method of SVM and spare Auto Encoder. The comparison with the previous study shows that SSAE (stacked sparse auto-encoder) performs well. DL method was used, extracting features from the proposed work. Binary And Multilevel classification is performed. S. Naseer et al. (2018) have compared the two different algorithms, namely, ML (Machine Learning) and DL (Deep Learning), with the help of the IDS algorithm. They have developed an anomaly model by RNN. The NSLKDD dataset trained this network. DL and ML techniques are compared by the well-known classification method. Finally, the experiment results are taken from the GPU-based test bed. M. Al-Qatf et al. (2018) have utilized the DL (Deep Learning) method to select features and reduce dimensionality. This process is helpful for training and testing the time and enhances the efficiency of SVM. They have also proposed an auto-encoder mechanism. This algorithm is used for feature representation, where features are fed into the SVM to enlighten the accuracy and intrusion capability. Based on the performance metrics results, SVM outperformed the other method. Non-linear dimensionality is used to control large-scale traffic data. N. Marir et al. (2018) have utilized SVM and deep feature extraction methods based on spark to detect the DOS attack in SDN. They have also used a DBN technique to extract the features. Then, the achieved features are fed to the multi-layer SVM. Compared with the earlier methods, the proposed results achieved better performance. H. Yao et al. (2018) proposed an IDS (Intrusion Detection System) framework involving four machine learning algorithms for cluster extraction, pattern discovery, classification, and updating. From the overall experiment compared with the other methods, MSML performs well. Finally, the accuracy and F1-score are estimated and compared in each module.

Sabeel et al. (2019) suggested that LSTM and DNN model predicts the input data's unknown Dos and DDOS files. And to evaluate the performance of the proposed model, the authors have generated a new set of datasets ANTS2019. The data collected from the CICIDS2017 datasets are trained using the proposed model to produce the final classification result. The analysis results indicate that the proposed DNN model classifies the DOS attacks in WSN with 99.68% accuracy. Wu et al. (2019) have proposed a hierarchal CNN and RNN model to detect the threats in the WSN system. The CNN and RNN model layers are combined and function to produce the final output. The result the evaluated using the UNSW-NB15 and NSL-KDD datasets. The evaluation results indicate that the proposed approach has achieved 99.36% and 99.05% accuracy on binary and multi-class classification, respectively. Shabban et al. (2019) suggested that the CNN model detects DDoS attacks in wireless sensor devices. Compared with other ML classifiers such as KNN, SVM, NN, and DT and with NSL-DD and simulated network traffic datasets, the proposed model classifies the attacks with 99% accuracy. But a single column is used to convert the data into the matrix, damaging the learning model. Vinayakumar et al. (2019) have developed a scalable hybrid DNN frame to monitor the load traffic and event to detect the cyber attack in DoS. The proposed model has achieved 99.2% accuracy for binary classification and 98.0% accuracy for multi-class classification. In order to find the efficiency of the proposed model, the KDD-99 dataset is applied with NSL-KDD, UNSW-NB15, WSN-DS, CICIDS2017, and Kyoto datasets.

G. Karatas et al. (2020) have used six ML methods to identify imbalanced and up-to-date datasets. They have concluded that the detection rate is increased. The ML methods are k-nearest, RF, Gradient Boosting, Adaboost, Decision tree, and LDA algorithm. SMOTE method is used to reduce the missed intrusion system and enhance efficiency. Based on the proposed method, performance data generation is used as a minor class. Haider et al. (2020) have proposed a CNN algorithm to detect the Dos attack in SDN. Various performance metrics are used to analyze the efficiency of the model. The experimental result shows that the proposed CNN model classifies the DoS files from the input data with 99.45% accuracy. But the main drawback is that the proposed model consumes more time to train and test the data. So, it may have possibilities of damaging the assaults. Kim et al. (2020) have developed a deep learning-based classifier CNN to detect and classify DoS attacks in WSN. The input data are gathered from two sets of datasets, such as KDD-99 and CICIDS2018, to perform the classification and process. To classify the input data, the CNN model converted the input data into a greyscale image and performed the classification process. The result of the CNN model is evaluated with the RNN algorithm. The comparison result showed that the CNN model more efficiently performs both binary and multi-class classification with 99% accuracy. Premkumar and

Sundararajan (2020) introduced a deep learning-based dense mechanism (DLDM) to detect DoS attacks in the data for-warding phase (DFP). The experimental result shows that the proposed model has achieved high PDR, throughput, and accuracy. The proposed model has detected flooding, jamming, fatigue, and homing attacks from the input datasets. Asad et al. (2020) proposed DNN based model to detect the intrusion in WSNs. It effectively classifies the types of DoS attacks from the input datasets. Through this model, various types of DoS attacks are identified. In order to improve the efficiency of the detection techniques, ML and DL algorithm is implemented.

Deshpande et al. (2021) evaluated the efficiency of five different machine-learning algorithms in detecting intrusion. The performance of each model is evaluated and compared with each other. Then K-fold cross-validation process is utilized to improve the accuracy result of the proposed approach. The final simulation result of the model indicates that the ML classifier RF and SVM and DL classifier ANN have performed better in detecting intrusions. Wazir Ali and Ahmad (2022) analyzed the efficiency of various ML algorithms in detecting the types of DoS attacks from the input data. The analysis results indicate that the J48 and RT models have performed better than the J48 model with less processing time and high speed. Salmi and Oughdir et al. (2022) proposed CNN and LSTM-based intrusion detection models to predict and classify various Dos attacks such as black holes, grey holes, TDMA, flooding, and Normal. In order to effectively classify the input datasets, the computer-generated wireless sensor network detection system is utilized. The result of the proposed approach shows that it exactly classifies the types of attack with 97% accuracy.

From the above discussions, it is noticed that many methods and techniques have been proposed for identifying and detecting DoS attacks in WSN. They were not discussing any unique architecture or the same environment. Different methods have been examined at different constraints, scenarios, and inputs. Thus, this paper has aimed to implement a few machine-learning algorithms for detecting DoS attacks in the NUSW-NB15_features.csv dataset and evaluate their performance. This paper used Decision Tree, Random Forest, Linear Regression, and Support Vector Machine algorithms for detecting DoS attacks in WSN.

III. MACHINE LEARNING ALGORITHMS

A few machine learning algorithms are simulated to find their betterness regarding DoS attack detection over network traffic data.

Logistic Regression

It uses the logistic function to classify the data. The logistic function varies with the application, and the sigmoid function is comprehensive as the logistic function for classification.

$$\boldsymbol{\phi}(\boldsymbol{z}) = \frac{\mathbf{1}}{\mathbf{1} + \boldsymbol{e}^{-\boldsymbol{z}}}$$

z represents the weights and features that are processed in a linear combination which is given below,

$$\boldsymbol{z} = \boldsymbol{w}^{\boldsymbol{T}}\boldsymbol{x} = \boldsymbol{w}_{\mathbf{0}} + \boldsymbol{w}_{\mathbf{1}}\boldsymbol{x} + \boldsymbol{w}_{\mathbf{2}}\boldsymbol{x}^{\mathbf{2}} + \ldots. + \boldsymbol{w}_{\boldsymbol{n}}\boldsymbol{x}^{\boldsymbol{n}}$$

The range of $\phi(z)$ is limited between the range [0,1]. If the z becomes plus infinity, the function outputs 1; if it becomes minus infinity, it becomes 0.

Decision Tree

The functioning of the decision tree is similar to that of humans making decisions on problems. It uses the classification for the prediction process. A decision tree has numerous branches, each leading to a possible value or a feature. Each node in the decision tree represents the test for a feature that leads to further data classification. This kind of classification algorithm helps in classifying unprocessed data.

Random Forest

It is similar to the decision tree algorithm. If a dataset with more features is considered, there is always the possibility of overfitting in decision tree algorithms. Random Forest is an ensemble learning algorithm with numerous decision trees, each with a weak classification and prediction. Those predictions are accumulated to form a single prediction that can give effective results.

SVM

It is a widely used supervised learning algorithm that uses classification and regression to classify the data. It finds the maximum separation between two data or the hyperplane separating them. The SVM algorithm finds the hyperplane for n-dimensional datasets and classifies them. Based on the size of the dataset and the number of features, the dimension of the plane varies. If there are two features, the plane becomes a single line; if there are three features, then the plane becomes 2-dimensional space.

Artificial Neural Network

It is a simulation of the functioning of a human brain that understands complex patterns and warns us. ANN is an extension of the biological neural network, which only accepts structured numeric data. Though most neural networks like CNN and ANN accept unstructured data, ANN can only accept structured data. An ANN model consists of three layers, input, hidden and output layers. They can also be termed as Multi-Layer Perceptron. The Hidden layer can also be termed a Distillation layer that extracts only the important patterns in them and forwards them to the succeeding layers. Only the important information is retained, and the redundant data are omitted at each layer. Finally, the extracted features are classified using an activation function. Several activation functions include sigmoid, tanh, ReLu, and ELU. The optimal weight W with minimum prediction error can be considered a successful prediction model. A back-propagation process converts ANN into a reinforcement algorithm that learns from its mistakes.

The machine learning algorithms are used and implemented in Python and experimented with the UNWS_NB dataset. The execution is carried out on Intel Pentium Core-i7, a 7th-generation processor. The HDD capacity is 1TB, and the RAM is 12 GB.

Dataset

One of the popular network traffic data, named UNSW_NB15, has eight categories of data, including features, testing, and training data. Each data has assigned a label as 0 or 1. If it is 1, then the data may belong to any one of the categories of {'Normal,' 'Reconnaissance,' 'Backdoor,' 'DoS,' 'Exploits,' 'Analysis.', 'Fuzzers' 'Worms' 'Shellcode' 'Generic'}. The entire dataset is divided into 80: 20 for training and testing processes. 23052 samples were taken for the training process, and 19760 samples were for the validation process. All the machine learning methods are assigned with a maximum of 300 epochs, and the accuracy, loss, and executions are estimated. The experimental results are compared with one another and shown in Figure-2.

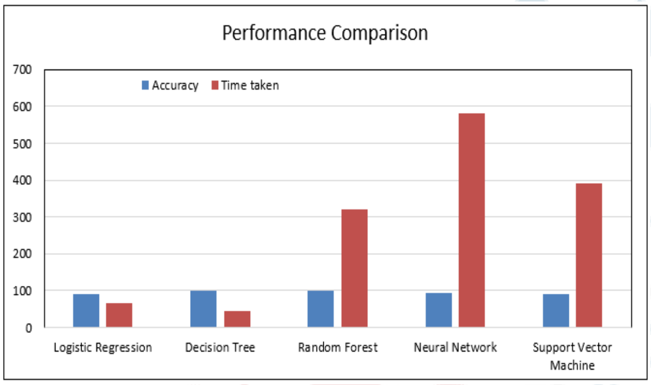

Figure-2. Performance Comparison

The comparison shows that the Decision Tree and Random Forest algorithms obtained the same accuracy of 99.74%. The Random Forest algorithm takes more epochs, and the decision tree takes fewer epochs. Hence, it is concluded that the DT algorithm is the better model for predicting DoS attacks from the network traffic dataset.

IV. CONCLUSION

WSNs are used in various real-time applications that are demanding worldwide. Real-time industries also attract it due to the growing advancements in sensors and technologies. Even though WSN has disadvantages regarding energy and security, this paper considers security the major problem and is motivated to design and implement a novel algorithm for automatice detection and prevention of DoS attacks. Before creating a new model, the has aimed to understand the issues and challenges of the earlier research works to create the problem statement. It carried out a detailed study on DoS attack detection using different algorithms in WSN and found that most of the mechanisms can identify the intrusion after data transmission in the network. After recording the data transmission functionality, the methods analyzed the network traffic data. Hence, it is essential to automatically identify and detect malicious nodes w.r.t DoS attacks in WSN using machine learning algorithms. Since machine learning algorithms can dynamically analyze the data, this paper implements four machine learning algorithms to verify their efficiency. From the comparison, it is found that the DT algorithm outperforms other algorithms.

In future work, an network simulation is done, and the dynamic data is analyzed using machine learning algorithms and find efficacy.

REFERENCE

[1] Shen, Y., Zheng, K., Wu, C., Zhang, M., Niu, X., & Yang, Y. (2018). An ensemble method based on the selection using bat algorithm for intrusion detection. *The Computer Journal*, *61*(4), 526-538.

[2] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on emerging topics in computational intelligence*, *2*(1), 41-50.

[3] Ali, M. H., Al Mohammed, B. A. D., Ismail, A., & Zolkipli, M. F. (2018). A new intrusion detection system based on a fast learning network and particle swarm optimization. *IEEE Access*, *6*, 20255-20261.

[4] Yan, B., & Han, G. (2018). Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system. *IEEE Access*, *6*, 41238-41248.

[5] Naseer, S.; Saleem, Y.; Khalid, S.; Bashir, M.K.; Han, J.; Iqbal, M.M.; Han, K. Enhanced network anomaly detection based on deep neural networks. IEEE Access 2018, 6, 48231–48246.

[6] Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. *Ieee Access*, *6*, 52843-52856.

[7] Marir, N., Wang, H., Feng, G., Li, B., & Jia, M. (2018). Distributed abnormal behavior detection approach based on deep belief network and ensemble SVM using spark. *IEEE Access*, *6*, 59657-59671.

[8] Yao, H., Fu, D., Zhang, P., Li, M., & Liu, Y. (2018). MSML: A novel multilevel semi-supervised machine learning framework for the intrusion detection system. *IEEE Internet of Things Journal*, *6*(2), 1949-1959.

[9] Karatas, G., Demir, O., & Sahingoz, O. K. (2020). Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. *IEEE Access*, *8*, 32150-32162.

[10] Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K. K. R., & Iqbal, J. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software-defined networks. *Ieee Access*, *8*, 53972-53983.

[11] Alsheikh, M. A., Lin, S., Niyato, D., & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms,

strategies, and applications. *IEEE Communications Surveys & Tutorials*, *16*(4), 1996-2018.

[12] Cheng, B., Cui, L., Jia, W., Zhao, W., & Gerhard, P. H. (2016). Multiple regions of interest coverage in camera sensor networks for tele-intensive care units. *IEEE Transactions on Industrial Informatics*, *12*(6), 2331-2341.

[13] Das, S., A. Abraham and B.K. Panigrahi, 2010. Computational intelligence: Foundations, perspectives and recent trends. Comput. Intell. Patt. Anal. Biol. Inform.

[14] Di, M., & Joo, E. M. (2007, December). A survey of machine learning in wireless sensor networks from networking and application perspectives. In *2007 6th International Conference on Information, communications & signal processing* (pp. 1-5). IEEE.

[15] Gavric, Z., & Simic, D. (2018). Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. *Ingeniería e Investigación*, *38*(1), 130-138.

[16] Mallikarjunan, K. N., Muthupriya, K., & Shalinie, S. M. (2016, January). A survey of distributed denial of service attack. In *2016 10th International Conference on Intelligent Systems and Control (ISCO)* (pp. 1-6). IEEE.

[17] Mazur, K., Ksiezopolski, B., & Nielek, R. (2016). Multilevel modeling of distributed denial of service attacks in wireless sensor networks. *Journal of Sensors*, *2016*.

[18] Ogbodo, E. U., Dorrell, D., & Abu-Mahfouz, A. M. (2017). Cognitive radio based sensor network in smart grid: architectures, applications, and communication technologies. *IEEE Access*, *5*, 19084-19098.

[19] Patil, A., & Gaikwad, R. (2015), "Comparative analysis of the prevention techniques of denial of service attacks in a wireless sensor network," *Procedia Computer Science*, *48*, 387-393.

[20] Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2010). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys & Tutorials*, *13*(2), 245-257.

[21] Rahman, M. A., Saleh, S. M., & Huq, S. M. (2017). Intrusion Detection System for Wireless ADHOC Network using Time Series Techniques. *International Journal of Computer Applications*, *975*, 8887.

[22] Shiaeles, S. N., Katos, V., Karakos, A. S., & Papadopoulos, B. K. (2012). Real-time DDoS detection using fuzzy estimators. *computers & security*, *31*(6), 782-790.

[23] Yu, Z., & Tsai, J. J. (2008, June). A framework of machine learning-based intrusion detection for wireless sensor networks. In *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008)* (pp. 272-279). IEEE.

[24] Abdullah, M. A., Alsolami, B. M., Alyahya, H. M., & Alotibi, M. H. (2018). Retracted: Intrusion detection of DoS attacks in WSNs using classification techniques. *Journal of Fundamental and Applied Sciences*, *10*(4S), 298-303.

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

[26] Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2020). Deepdetect: detection of distributed denial of service attacks using deep learning. *The Computer Journal*, *63*(7), 983-994.

[27] Deshpande, S., Gujarathi, J., Chandre, P., & Nerkar, P. (2021). A Comparative Analysis of Machine Deep Learning Algorithms for Intrusion Detection in WSN. *Security Issues and Privacy Threats in Smart Ubiquitous Computing*, 173-193.

[28] Gunduz, S., Arslan, B., & Demirci, M. (2015, December). A review of machine learning solutions to denial-of-services attacks in wireless sensor networks. In *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)* (pp. 150-155). IEEE.

[29] Kim, J., Kim, J., Kim, H., Shim, M., & Choi, E. (2020). CNN-based network intrusion detection against denial-of-service attacks. *Electronics*, *9*(6), 916.

[30] Lee, B., Amaresh, S., Green, C., & Engels, D. (2018). Comparative study of deep learning models for network intrusion detection. *SMU Data Science Review*, *1*(1), 8.

[31] Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *Ieee Access*, *6*, 3491-3508.

[32] Park, T., Cho, D., & Kim, H. (2018, July). An effective classification for DoS attacks in wireless sensor networks. In *2018 Tenth international conference on Ubiquitous and future networks (ICUFN)* (pp. 689-692). IEEE.

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

[34] Sabeel, U., Heydari, S. S., Mohanka, H., Bendhaou, Y., Elgazzar, K., & El-Khatib, K. (2019, December). Evaluation of deep learning in detecting unknown network attacks. In *2019 International Conference on Smart Applications, Communications and Networking (SmartNets)* (pp. 1-6). IEEE.

[35] Salmi, S., & Oughdir, L. (2022). CNN-LSTM Based Approach for Dos Attacks Detection in Wireless Sensor Networks. *International Journal of Advanced Computer Science and Applications*, *13*(4).

[36] Shaaban, A. R., Abd-Elwanis, E., & Hussein, M. (2019, December). DDoS attack detection and classification via Convolutional Neural Network (CNN). In *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)* (pp. 233-238). IEEE.

[37] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for the intelligent intrusion detection system. *Ieee Access*, *7*, 41525-41550.

[38] Wazirali, R., & Ahmad, R. (2022). Machine learning approaches to detect DoS and their effect on WSNs lifetime. *Comput. Mater. Contin*, *70*(3), 4922-4946.

[39] Wu, P., Guo, H., & Buckland, R. (2019, March). A transfer learning approach for network intrusion detection. In *2019 IEEE 4th international conference on big data analytics (ICBDA)* (pp. 281-285). IEEE.