A Deep Learning Model For Efficient Intrusion Detection In Wireless Sensor Networks

A Subhash
Department of Computer Science
Dr NGP Arts and Science College, Coimbatore, India.
asubhash.itworld@gmail.com
C Kumuthini
Department of Computer Applications, Dr NGP Arts and Science College,Coimbatore,India.
kumuthini@drngpasc.ac.in

Abstract:
The application of WSN has been rapidly growing in the field of agriculture, security, and manufacturing industry and healthcare. Sensors deployed in remote areas are difficult to reach and the resources such as power, storage, signal strength and communication range are constrained which makes the network to be vulnerable to different attacks and exploitations. WSN face security threats as the network is resource constrained due to establishment in hostile environment. Intrusion detection system plays an important role in mitigating WSN exploitations and attacks. Denial of Service (DoS) is the most common type of attack in WSN which disrupts the network functionality and affect sensor data. To efficiently detect intrusions and anomalies in WSN, a light weight deep learning model is proposed to detect different types of attacks. The performance of the proposed intrusion detection model is compared with state-of-art machine learning models. The performance of the proposed model demonstrated higher detection accuracy of different types of attacks in WSN.
Keywords: Intrusion detection in WSN, DOS attacks, deep learning, anomaly detection

DOI: 10.24297/j.cims.2024.08.4

1. Introduction

Wireless sensor networks are utilized in various fields such as military, healthcare, environmental, manufacturing for application that ranges from tracking, surveillance, monitoring and collection of data. A Wireless Sensor Network (WSN) consists of very small sensors which are interconnected through wireless communication and are deployed to read, monitor and collect data from the surroundings. The performance of a WSN depends on the network lifetime and resource management. Sensors deployed in remote areas are difficult to reach and the resources such as power, storage, signal strength and communication range are constrained which makes the network to be vulnerable to different attacks and exploitations (Gowdhaman and Dhanapal, 2022).

Misuse detection and anomaly detection are the two types of detection methods that are widely used to filter and detect intrusions (Depren et al., 2005) in WSN. Misuse detection exactly matches the stored signatures and ignores the patterns that newly arise while anomaly detection matches the deviations that differ from the normal behavior. Anomalies are malicious or those that are compromised nodes which perform malicious activities affecting the network (Lai et al., 2022). To detect and isolate malicious nodes researchers used authentication schemes (Xiong, et al., 2019) and proposed various methods to detect nodes that are compromised (Sert et al., 2017). Malicious nodes attacks are targeted towards the data collected in the network and are destroyed. Therefore intrusion detection system (IDS) should be capable of capturing not only known signatures but also unknown patterns (Otoum & Nayak, 2021). Denial-of-Service (DOS) is the most common form of attacks in WSN which floods the communication channel with repeated requests and hinder sending and receiving of messages (Gill et al., 2009).

WSN collects different types of data pertaining to the environment deployed and faults in the sensor node could affect the overall network performance and network lifetime. In the resource constrained network, identifying nodes with faults is important to improve the network performance and to reduce the risk of sensor network failure (Wang et al., 2020). Machine learning technique offers state of art methods to classify, predict, derive rules, group data and learn patterns present inside the data to make intelligent decisions. Machine learning techniques are employed for WSN problems such as fault diagnosis, routing, intrusion detection, data aggregation etc (Wazirali & Ahmad, 2022).

The random deployment of sensor nodes in WSN causes several problems like security issues, poor data aggregation, poor authentication and nodes become malicious despite improvement in node coverage, increased neighboring nodes and maximize network connectivity (Abo-Zahhad et al., 2015; Priyadarshi et al., 2020). The presence of malicious nodes cause energy depletion, send false data, alter data aggregation cycles and affects the overall WSN life time. To extend the WSN network lifetime, it is necessary to identify and isolate the malicious nodes from the network. Also the techniques employed to detect malicious node must be capable of capturing different unknown patterns (anomalies) instead of known patterns (signatures). For anomaly detection different machine learning models are currently being studied for their higher detection rate. Machine learning models do suffer from scalability as network data is comprised of large number of features and large volume of network data which needs a sophisticated method to utilize vast amount of data with higher detection rate. Also, it is equally important to indentify the type of attacks to take corrective actions against the attacks in WSN.

In DOS attack the services of sensor node or Base Station or Cluster Heads are denied so that the network operates incorrectly. Some of the indications of DOS attack include reduction in the network performance, poor responsiveness from a particular area of the network, sudden increase in messages and increase in packet loss. Also, the WSN is resource constrained, power, storage, signal strength and communication range are limited. Therefore building an intrusion system for resource constrained network that is less expensive on computation, storage and highly efficient in intrusion detection is the primary requirement to mitigate attacks and anomalies in WSN. Motivated by aforementioned problems the present work proposes a light weight deep learning model to effectively classify malicious and normal nodes using large number of features and network data with high detection rate. The present work also provides related works on the methods used to detect malicious nodes in the WSN. The proposed deep learning model performance is compared against other methods used in the literatures for high detection rate.

The present work contributes to understand feature information and make use of feature information for detection of different attacks in WSN. Since features may contain redundant data, ignoring those features and utilizing informative feature will enhance the detection accuracy. The main contribution of the proposed work is to utilize automatic feature learning and make accurate decisions on malicious nodes, and to uncover hidden patterns relative to different types of attacks involved in Denial of service in WSN. A comparative analysis is also carried out with state-of-art machine learning models and the proposed model is evaluated using performance metrics such as accuracy, F1-socre, precision and recall.

The present work is organized into five sections. Introduction to intrusions in WSN is present in section one, section two presents related work, section three presents the methodology of the proposed model, section four discusses experiment and analysis, section five presents the results and discussion and finally concludes the paper.

2. Related Works

This section discuses some of the related literature's about intrusion detection in WSN. The related work explores the detection method employed, the performance of the model in detecting WSN attacks in general and particular to WSN-DS dataset.

(Talukder et al., 2024) proposed a data balancing technique to improve the performance of IDS. The dataset is balanced using SMOTETomeLinks which remove the noises in the majority class and uniformly distributes the classes. This techniques improved classifiers performance in binary

and multi-class problem. On WSN-DS dataset, the performance of the machine learning models such as DT, RF, MLP, KNN, LGB and XGB considerably improved to 99% when SMOTETomeLinks is applied.

(Salmi & Oughdir, 2023) developed different deep learning models for intrusion detection system to detect DOS attacks. Single layer Dense neural network, Convolution neural network, Recurrent neural network and a combination of CNN and RNN network models are trained using WSN DOS attack dataset. CNN achieved highest accuracy of 98.79% over other models while RNN and combined RNN+ CNN models achieved accuracy less than 97%.

(Lai et al., 2023) proposed an online learning technique to detect DOS attack in WSN. Using feature selection the performance of the online classifier is enhanced. A modified Genetic algorithm with Maximum information coefficient (MIC) is used to extract the features and the extracted features are classified using multi-class passive-aggressive method. The proposed model achieved an accuracy of 97.16% outperforming SVM, DT, MPA and MPA II. The proposed model demonstrated that feature selection improves model performances.

(Singh et al., 2024) proposed an intrusion detection and prevention system using CNN model. The proposed CNN is constructed using SS linear scaling Adam optimizer. The proposed model is trained using CIC Dos dataset and the model achieved a highest accuracy of 98.15% over CNN, ANN and RNN models. The soft swish function is used instead of Softmax layer to regulate the training speed of the network and the model efficiently classified intrusions.

(Tabbaa et al., 2022) proposed an ensemble model consisting of homogeneous and heterogeneous models. Homogeneous models consist of several instances of base learner while heterogeneous models include adaptive random forest (ARF), NB, Hoeffding adaptive tree (HAT). The proposed ensemble model is tested on WSN-DS dataset and both models performed well with highest accuracy of more than 96% and 97% for intrusion detection in WSN.

(Alruhaily & Ibrahim, 2021) proposed a multi layer intrusion detection system in which NB classifier is used on the network edge sensors and RF is used to further classify the type of intrusions. Using mutual information, the features are selected and the selected features are used to classify the traffic. In the second step, RF is used to differentiate the type of intrusion in the traffic data. Compared with existing models, the proposed model achieved a highest average accuracy of 97.3%.

(Ifzarne et al., 2021) proposed real time anomaly detection model to detect DOS attacks in WSN. The proposed system employed feature selection using information gain ratio and using passive aggressive algorithm the anomalies are classified. The proposed model is tested against info gain and chi-square feature selection methods using different classifiers. The proposed information gain ratio and PA algorithm achieved 96% of accuracy compared to other passive learner's for anomaly detection in WSN.

(Almomani & Alenezi, 2018) investigated different machine learning algorithms on a newly derived WSN dataset for DOS attacks. To reduce the computational complexity, the author applied feature selection before classifying different DOS attacks. The accuracy of machine learning model reach to 98% while reducing features to about 53%.

(Vinayakumar et al., 2019) proposed a deep neural network and the performance of the proposed method is evaluated using CICIDS2017, WSN-DS, Kyoto, UNSWNB, NSL-KDD and KDDCUP. Different architecture layer size from 1 to 5 is evaluated on multi-class classification WSN-DS. DNN with1 layer achieved a highest accuracy of 98% while DNN with 5 layers achieved 96% and DNN with 3 layers achieved 97% accuracy on WSN-DS. Compared to other machine learning models, RF achieved a highest accuracy of 99%.

(Ben Atitallah et al., 2022) investigated the transfer learning model for DOS attacks in WSN. The proposed method combined majority voting method with the transfer learning models. The proposed ensemble model achieved highest accuracy on DOS attack detection but the model is computationally expensive to address the resource constrained WSN.

3. Methodology

3.1 Convolution Neural Network

A convolution neural network consists of input layer or convolution layer, sub sampling layer, activation, pooling, fully connected layer and output layer. The input layer contains convolution filters and the convolution filters is made up of mathematical operations which yields an output function from a set of functions x and y. The input vector X represents the network features and the convolution filters learns from the set of functions f(x,y) and maps the input feature X to the target class C. The target class C for intrusion detection represents the types of DOS attacks in WSN.

The input vector X for network features is given by

$$X = \{x_1, x_2, x_3 x_4 \ldots x_n\} \quad (1)$$

Then, the output of the convolution filter is given by

$$O[X] = f(x,y)[X] \quad (2)$$

$$O[X] = f(x,y)\left(\sum_{i=1}^{p} X_i^{1-1} w_{ij}^1 + b_j^1\right) \quad (3)$$

where p is the number of convolution filters in layers 1-1 and w_{ij}^1 is the weight in the ith and jth neuron in layer 1-1. b_j^1 represents the bias of the jth neuron in the layer 1 and f(x,y) is the activation function. The input X is represented in matrix and the matrix is referred to kernel. The kernel moves in one direction for 1DCNN and moves in two directions for 2DCNN. The convulsion filters learns the input signal and maps to the corresponding target class C for reference. The input for a particular attack type reference is convoluted in the input kernel and passed on to the next layer as output signal.

To limit the number of output from the convolution filters, a non linearity is introduced through activation functions. ReLU, Sigmoid and tanh are the three non linearity functions applied in CNN. ReLU activation function is more efficient than tanh and Sigmoid as it converges faster. The ReLu function is given by,

$$ReLU\ (X) = \begin{Bmatrix} 0, X \leq 0, \\ X, X > 0 \end{Bmatrix} \quad (4)$$

After convolution layers, pooling layers are introduced to reduce the dimension of input vector. In the pooling layer the features with maximum information are retained while features with poor information are dropped often referred to down-sample. Max pooling and average pooling are the two types of pooling functions used in classification problem. Average pooling is given by (Yu et al., 2014) and it reduces the feature dimension through selecting a small region and averages its values.

$$f_{\text{avg}\,(X)} = \frac{1}{\mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{X_i} \quad (5)$$

Max pooling reduces the feature dimension through selecting maximum values in a small region. Max pooling is given by (Graham, 2014)

$$f_{\max\,(X)} = \max\{X_i\}_{i=0}^{N} \quad (6)$$

The next layer is the fully connected layer, where feature vector is flattened. The fully connected layer represents that all the layers between input layer and output layers are fully connected. The output vector is returned as a dot product of weights and the input vector is given as,

$$[Out_X] = b+w_1X_1+w_2X_2+....w_nX_n \quad (7)$$

where w is the weights, X is the input feature vector and n is the number of features in the input vector. To convert the output vector to prediction probabilities, softmax function is applied which returns the probabilities of each target class. The softmax function is given by,

$$\text{Softmax (x)} = \frac{e^x}{\sum_{j=1}^{k} e^x} \quad (8)$$

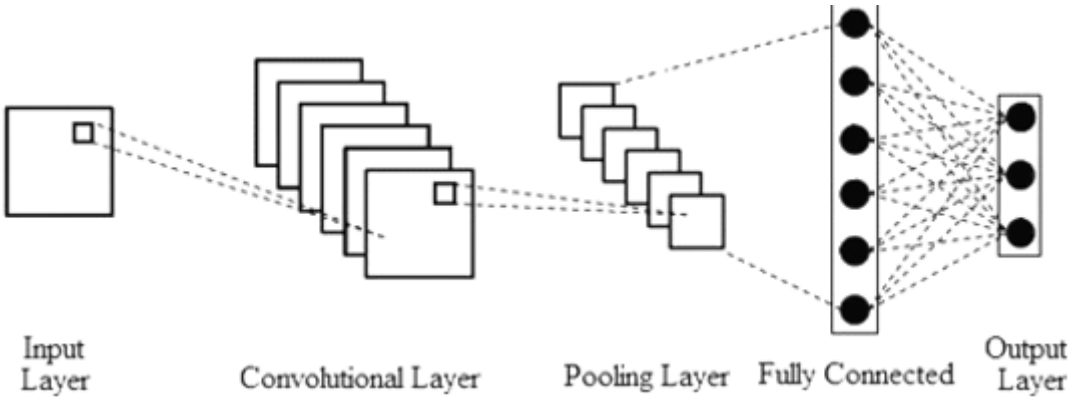

Figure 1 Typical CNN Layer

3.2 Proposed Methodology

Convolution Neural Networks are complex and have computational complexities where as WSN are resource constrained. In order to utilize our proposed CNN model for intrusion detection in resource constrained WSN, the proposed model is kept light weight. To detect intrusion in WSN, a CNN model is developed using three convolution layers. The proposed CNN model consists of input layer, three convolution layer and output layer (Table 1). The input layer consists of 64 neurons, kernel size of 1 x 1 and input dimension of 17 with ReLU activation. The second convolution layer consists of 32 neurons with kernel size of 1 x 1 with ReLU activation. A dropout layer (0.2) is added to the second convolution layer to reduce the data dimension and helps in preventing overfitting. The third convolution layer consists of 32 neurons and kernel size of 1 x 1 with ReLU activation. The output layer consists of dense 5 neurons with softmax activation. The proposed CNN model is designed to be light weight for resource constrained WSN and has a total of 4,453 trainable parameters. There is a trade-off between computational complexity and prediction accuracy. Adding more layers and filters may increase in more feature extraction which causes the network to overfit resulting in increased false positives. Also the number of trainable parameters increases with increase in layers as result of increased weights and therefore the computational complexity increases. Less number of layers and kernels allows the network to extract and learn complex features at each layer will help to improve the prediction accuracy (Al Shoura et al., 2023). Utilizing automatic feature selection removes the limitations of filter, wrapper

and embedded methods and offers an advantage of correlating features which can be ignored in supervised feature selection methods. Automatic feature learning characteristics of a CNN model has several advantages over supervised feature learning methods as anomalies and attack patterns that change constantly. Automatic feature learning helps in understanding different patterns of attacks and helps to mitigate known attacks and unknown attacks in future. Secondly, automatic feature learning can help prediction models to adapt to evolving attacks and offer better predictive performance. The architecture of the proposed approach is given in Figure 2.

Table 1 Proposed CNN Model Summary

Model	Layer	Output shape	Parameters
CNN	Conv2d	(None, 64)	1152
	Conv2d	(None, 32)	2080
	Dropout	(None, 32)	0
	Conv2d	(None, 32)	1056
	Flatten	(None, 32)	0
	Dense	(None, 5)	165
Total Params: 4,453 Trainable Params: 4,453 Non trainable params: 0			

Algorithm for CNN attack detection

Input: Xi (network features), yi (target class)

Output: target class prediction yi (target class)

1. Preprocess Xi (scalar transformation)

2. Define evaluation metrics using TP, FP, TN, FN

2. Split input Xi into train set and test set

3. Build CNN architecture with 1 input layer, 3 convolution layer (1 x 1) and 1 output layer, Activation = relu & activation = softmax , Dropout=0.2

4. Compile CNN model (optimizer = adam, learning rate =0.001 and activation = 'softmax', loss=categorical_crossentropy)

5. Fit model using train set

6. Validate model using test set
7. Evaluate CNN model using evaluation metrics
8. Return evaluation metrics

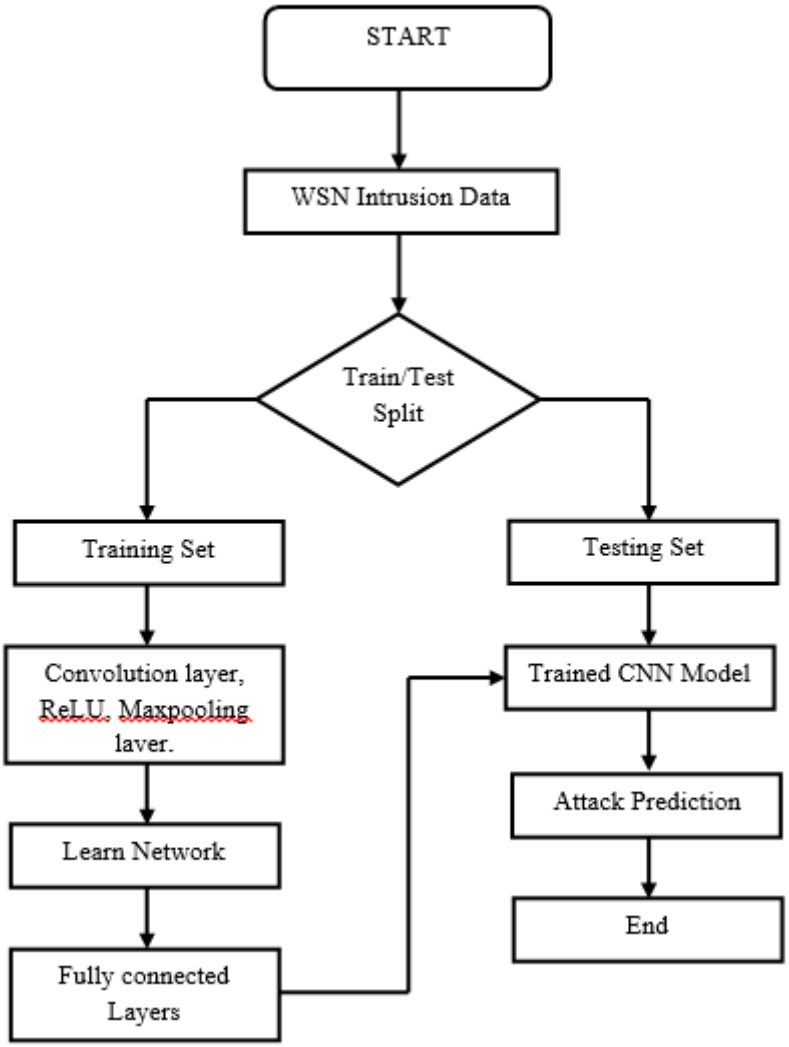

Figure 2 Architecture of the proposed approach

4. Experiment and analysis

4.1 Dataset

The proposed CNN model for intrusion detection in WSN is evaluated using WSN-DS dataset (Almomani et al., 2016). The dataset contains a total of 374661 instances with four types of attacks and eighteen features. The details of the features are listed in Table 2. The attack type includes blackhole, flooding, grayhole and TDMA. In Blackhole attack, the packets are not forwarded to sink node and they are dropped by the attacker. In Grayhole attack, the attacker broadcast as a CH and the attacker selectively discards the data packet and prevent forwarding packets when the attacker receives data from its members. In Flooding attack, once the CH is compromised it sends

advertising messages to its members in a large scale to consume more power, energy and traffic. In TMDA, the attackers set a schedule to broadcast all the nodes at a same time leading to data loss. The WSN-DS dataset contains 10050 instances of Blackhole attack, 3312 instances of Flooding attack, 14596 instances of Grayhole attack, 6638 instances of TDMA and 340066 instances of normal. The feature details are given in Table 2. All the experiments are conducted in Windows 10 pro machine with Intel(R) Core (TM) i3-CPU @2.00GHz with 8GB installed RAM, 3.6 python library, Anaconda Programming framework with Tensor flow. The WSN-DS dataset is split into training set and testing set in the ratio of 80:20. The training set contains 299728 instances and testing set contains 74933 instances.

Table 2 Features present in WSN-DS dataset

Feature Name	Feature details	Description
id	Node Id	A unique ID number of the sensor node
Time	Time	The run-time of the node in the simulation
Is_CH	Is CH	Describes if the node is a CH or not
Who_CH	Who CH	Cluster head ID
Dist_To_CH	Distance to CH	Distance between node and CH
ADV_S	ADV CH sends	Number of the advertise CH's broadcast messages sent to nodes
ADV_R	ADV CH receives	Number of advertise messages received by the nodes from CH
JOIN_S	Join request send	Number of join request messages sent by the nodes to the CH
JOIN_R	Join request receive	Number of join request messages received by CH from nodes
SCH_S	ADV SCH	sends messages of TDMA schedule broadcast sent to the nodes
SCH_R	ADV SCH receives	Number of scheduled messages received by the CH
Rank	Rank	Node order in TDMA scheduling
DATA_S	Data sent	Number of data packets sent from the node to its CH
DATA_R	Data received	Number of data packets received by the node from the CH
Data_Sent_To_BS	Data sent to BS	Number of data packets that are sent from node to the BS
Dist_CH_To_BS	Distance CH to BS	Distance between CH and BS
Send_code	Send code	The sending code of the cluster
Consumed_Energy	Energy consumption	Energy consumed
Attack_type	Attack type	Type of attacks or normal trac

4.2 Evaluation Metrics

The proposed approach is evaluated by comparing with state-of-art machine learning methods using metrics such as accuracy, precision, recall and f1-score. The evaluation metrics are derived

from the confusion matrix (Table 3). A confusion matrix summarizes the performance of a classification model using TP, TN, FP and FN. True Positive (TP) are the instances that are true and correctly classified as true. True Negatives (TN) are the instances that are False and correctly classified as False. False Positives (FP) are the instances that are actually true but incorrectly classified as false. False Negatives (FN) are the instances that are actually false and incorrectly classified as True. Accuracy, recall, precision and F1-score is given by

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

$$\text{Recall} = \frac{TP}{TP+FN}$$

$$\text{Precision} = \frac{TP}{TP+FP}$$

$$\text{F1-score} = \frac{2TP}{2*TP + (FP+FN)}$$

Table 3 Confusion Matrix

		Predicted: Positive	Predicted: Negative
Actual	Positive	True Positive TP	False Positive FP
	Negative	False Negative FN	True Negative TN

5. Results and Discussion

The proposed model is evaluated on WSN-DS dataset and the performance of the proposed approach is compared against Random Forest (RF), Support vector machine (SVM), Linear Discriminant Analysis (LDA), Logistic regression (LR), and Extreme Gradient boosting (XGB). Using WSN-DS training set, RF, SVM, LDA, LR and XGB models were trained and using testing set, the models are tested for their performances in predicting different attack types. The metrics include accuracy, recall, precision and F1-score were calculated. The performance metrics for all the machine learning models are given in Table 4.

Table 4 Performance of different algorithms for attack prediction

Methods	Precision	Recall	F1-score	Accuracy

RF	99%	98%	98%	98%
SVM	98%	98%	98%	98%
LDA	97%	96%	96%	96%
LR	97%	97%	97%	97%
XGB	99%	98%	98%	98%
DT	97%	96%	96%	96%
Proposed CNN	**99%**	**99%**	**99%**	**99%**

According to Table 4, the proposed CNN model outperformed all other machine learning models with a highest accuracy of 99% while RF, SVM and XGB reached accuracy of 98%, LR reached 97% accuracy while LDA and DT recorded a lowest accuracy of 96%. In terms of precision, proposed model, RF and XGB reached 99% while SVM outperformed LDA, DT and LR with precision of 98%. LDA, DT and LR achieved a lowest precision of 97%. For recall, the proposed model outperformed all other models with recall of 99%. XGB, SVM and RF reached recall value of 98% while LR reached 97%. DT and LDA reached lowest recall value of 96%. For F1-Score, the proposed model achieved 99% outperforming other models while RF, SVM and XGB produced F1-score of 98% outperforming DT, LR and LDA (96%). The performance of the proposed CNN model on different attack types is given in Table 5.

Table 5 Proposed CNN Results

Attack types	Precision	Recall	F1-score
Normal	1.00	1.00	1.00
Blackhole	0.92	1.00	0.96
Flooding	1.00	0.92	0.96
Grayhole	0.90	0.85	0.87
TDMA	0.80	0.88	0.84
Weighted Avg	**0.99**	**0.99**	**0.99**
Overall Accuracy		**0.99**	

The proposed CNN model for Blackhole attack type achieved precision of 92%, recall of 100% and f1-score of 96%. For Flooding attack, the proposed model's precision reached 100%, recall of 92% and F1-score reached 96%. For Grayhole attack, the proposed model achieved precision of 90%, recall of 88% and F1-score of 87%. For TDMA attack, the model achieved precision value of 80%, recall of 88% and F1-score of 84%. The performance of the proposed model is superior in terms of weighted average precision of 99%, recall of 99% and F1-score of 99% and overall accuracy of 99% over other models. Precision measures the model's prediction quality towards positive cases, in intrusion detection, the main goal is to establish a network flow is normal in the first place and

high precision demonstrate that the model is correctly predicting positive cases. The proposed model achieved 100% of precision for normal and Flooding attack, 92% for Blackhole, 90% for Grayhole and 80% for TDMA and weighted average precision is 99%.

Recall measure the model ability to classify positive cases. Higher recall shows the model classification power to classify positive cases as positive. The recall rate for normal class is 100% which indicates that the proposed model is correctly classifying positive cases. The recall for Blackhole attack is 100%, for Flooding is 92% and for TDMA is 88% and the weighted average recall is 99%. The lower precision and recall value for Blackhole, Grayhole and TDMA corresponds to the low number of instances compared to other attack types. F1 score harmonize precision and recall and it is very important metric to consider for multi-class classification as there is a trade-off between precision and recall during class imbalance. The weighted average F1 score of the proposed model is 99% which indicates that the proposed model has a good balance in classifying positive and negative classes.

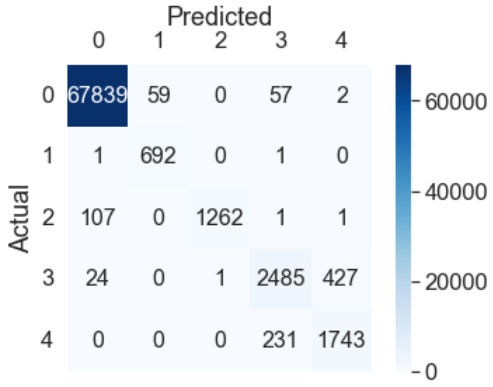

Figure 3 Confusion Matrix of the proposed model

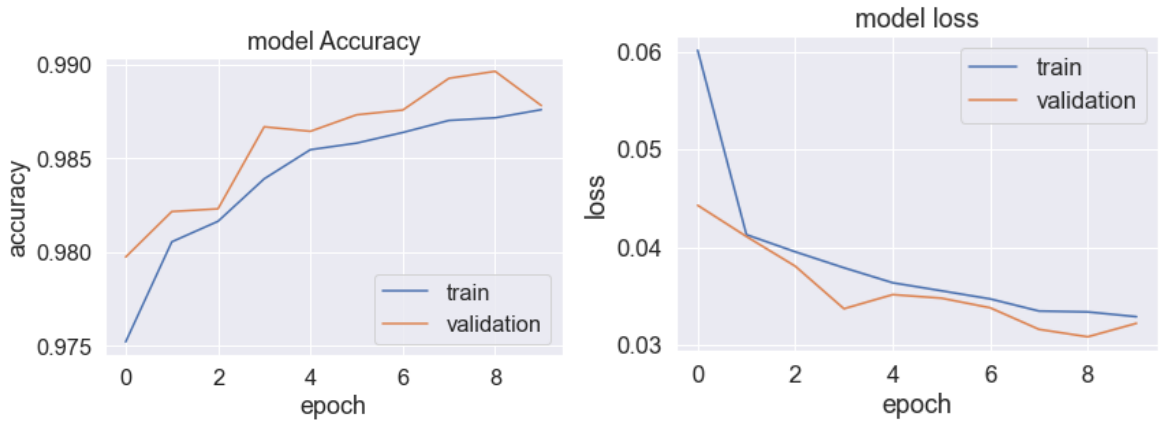

Figure 4 Accuracy and Loss curve on WSN-DS dataset

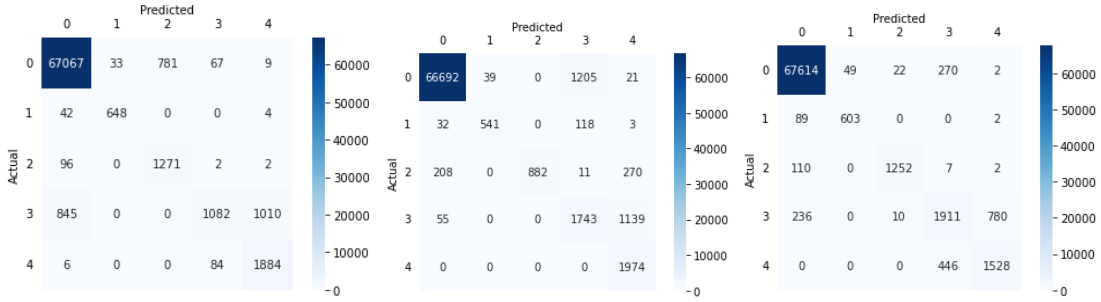

Figure 5 Confusion Matrix for DT, LDA and LR

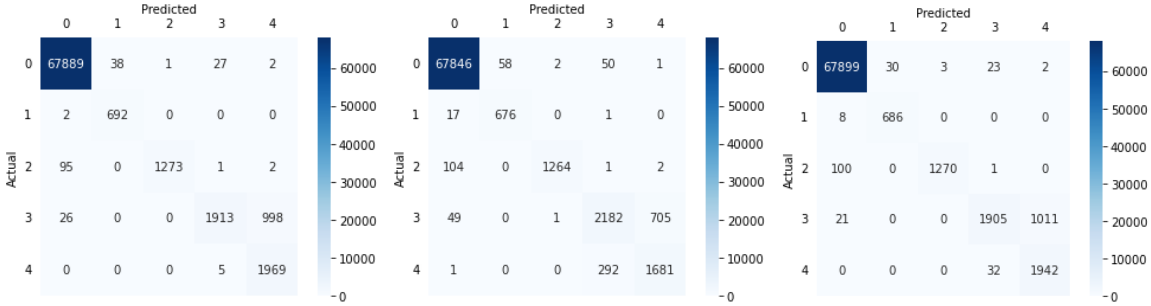

Figure 6 Confusion Matrix for RF, SVM and XGB

To demonstrate the efficiency of the proposed model, the performance of the proposed approach is compared with state-of-art machine learning models. The confusion matrix for DT, LDA, and LR is given in Figure 5 and the confusion matrix for RF, SVM and XGB is given in Figure 6. The proposed CNN model is constructed using an input layer, two convolution layers and a dense output layer. The proposed model is kept light-weight as WSN is resource constrained. The proposed model achieved higher accuracy of 99% than CNN model proposed by (Salmi & Oughdir, 2023). In GA-MIC method proposed by (Lai et al, 2023) the features are selected using a supervised method which improved the accuracy but CNN models are robust in automatic feature learning using weight sharing scheme. Compared to single layer, five layer and three layer CNN models proposed by (Vinaykumar et al., 2021) our proposed model achieved higher accuracy rate. Optimizing hyper parameters in CNN models is challenging and achieving right combination of hyper parameter tuning improves CNN model performance. Dropout and regularization techniques are useful to avoid overfitting and higher dropout rate will diminish the feature information. The proposed model demonstrated superior automatic feature learning over (Tabbaa et al., 2022), (Alruhaily & Ibrahim, 2021) and (Ifzarne et al., 2021) methods that adopts supervised feature selection. The validation loss and validation accuracy is illustrated in Figure 4 which depicts that model is stable at each epoch and not over fitting as the loss minimizes with the training and the accuracy is higher with training which indicates accurate predictions of the model.

Table 6 comparison of proposed model with machine learning models

Author	Year	Method	Accuracy%
Salmi & Oughdir,	2023	CNN	98.79%
Lai et al.,	2023	GA-MIC	97.16%
Tabbaa et al.,	2022	ARF,HAT	ARF-96%, HAT-97%
Alruhaily & Ibrahim,	2021	RF+MI	97.3%
Ifzarne et al.,	2021	CS+PAA	96%
Vinayakumar et al.,	2021	1LDNN,5LDNN, 3LDNN	1LDNN-98%, 5LDNN-96%, 3LDNN-97%
Proposed	**2024**	**3LCNN**	**99%**

6. Conclusion

Since WSN are resource constrained, the network is prone to different attacks and exploitations. WSN security is essential to keep the network functioning with adequate security but resource limitations and constraints are the challenges. In this paper, a light weight CNN model is proposed to detect the attack types and anomalies in resource constrained WSN. The performance of the proposed approach is evaluated using WSN-DS dataset. The findings of the study suggests that deep learning based intrusion detection showed higher detection rate of malicious attacks in WSN. The study confirmed that the performance of the proposed model is efficient and outperformed RF, SVM, LDA, LR, DT and XGB models with 99% of accuracy, 99% of precision, 99% of recall and 99% of F1-score. Also, the proposed model is trained and tested on a single dataset and as a future work; the proposed model will be evaluated on different datasets for different attack types.

References:

1. Abo-Zahhad, M., Ahmed, S. M., Sabor, N., & Sasaki, S. (2015). Rearrangement of mobile wireless sensor nodes for coverage maximization based on immune node deployment algorithm. Computers & Electrical Engineering, 43, 76-89.
2. Al Shoura, T., Leung, H., & Balaji, B. (2023). An Adaptive Kernels Layer for Deep Neural Networks Based on Spectral Analysis for Image Applications. Sensors, 23(3), 1527.
3. Almomani .I , B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: a dataset for intrusion detection systems in wireless sensor networks," Journal of Sensors, vol. 2016, p. 16, 2016.
4. Almomani, I. M., & Alenezi, M. (2018). Efficient Denial of Service Attacks Detection in Wireless Sensor Networks. J. Inf. Sci. Eng., 34(4), 977-1000.
5. Alruhaily, N. M., & Ibrahim, D. M. (2021). A multi-layer machine learning-based intrusion detection system for wireless sensor networks. International Journal of Advanced Computer Science and Applications, 12(4), 281-288.

6. Ben Atitallah, S., Driss, M., Boulila, W., & Almomani, I. (2022, September). An effective detection and classification approach for dos attacks in wireless sensor networks using deep transfer learning models and majority voting. In International Conference on Computational Collective Intelligence (pp. 180-192). Cham: Springer International Publishing.
7. Depren, O., Topallar, M., Anarim, E., & Ciliz, M. K. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert systems with Applications, 29(4), 713-722.
8. Gill, K., & Yang, S. H. (2009, November). A scheme for preventing denial of service attacks on wireless sensor networks. In 2009 35th Annual Conference of IEEE Industrial Electronics (pp. 2603-2609). IEEE.
9. Gowdhaman, V., and R. Dhanapal. "An intrusion detection system for wireless sensor networks using deep neural network." Soft Computing 26.23 (2022): 13059-13067.
10. Graham, B. (2014). Fractional max-pooling. arXiv preprint arXiv:1412.6071.
11. Ifzarne, S., Tabbaa, H., Hafidi, I., & Lamghari, N. (2021). Anomaly detection using machine learning techniques in wireless sensor networks. In Journal of Physics: Conference Series (Vol. 1743, No. 1, p. 012021). IOP Publishing.
12. Lai, T. T., Tran, T. P., Cho, J., & Yoo, M. (2023). DoS attack detection using online learning techniques in wireless sensor networks. Alexandria Engineering Journal, 85, 307-319.
13. Lai, Y., Tong, L., Liu, J., Wang, Y., Tang, T., Zhao, Z., & Qin, H. (2022). Identifying malicious nodes in wireless sensor networks based on correlation detection. Computers & Security, 113, 102540.
14. Otoum, Y., & Nayak, A. (2021). As-ids: Anomaly and signature based ids for the internet of things. Journal of Network and Systems Management, 29(3), 23.
15. Priyadarshi, R., Gupta, B., & Anurag, A. (2020). Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues. The Journal of Supercomputing, 76, 7333-7373.
16. Salmi, S., & Oughdir, L. (2023). Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. Journal of Big Data, 10(1), 17.
17. Sert, S. A., Fung, C., George, R., & Yazici, A. (2017, July). An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks. In 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE) (pp. 1-6). IEEE.
18. Singh, V. K., Sivashankar, D., Kundan, K., & Kumari, S. (2024). An Efficient Intrusion Detection and Prevention System for DDOS Attack in WSN Using SS-LSACNN and TCSLR. Journal of Cyber Security and Mobility, 135-160.

19. Tabbaa, H., Ifzarne, S., & Hafidi, I. (2022). An online ensemble learning model for detecting attacks in wireless sensor networks. arXiv preprint arXiv:2204.13814.
20. Talukder, M. A., Sharmin, S., Uddin, M. A., Islam, M. M., & Aryal, S. (2024). MLSTL-WSN: Machine Learning-based Intrusion Detection using SMOTETomek in WSNs. arXiv preprint arXiv:2402.13277.
21. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. Ieee Access, 7, 41525-41550.
22. Wang, M., Lu, Y., & Qin, J. (2020). A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Computers & Security, 88, 101645.
23. Wazirali, R., & Ahmad, R. (2022). Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime. Computers, Materials & Continua, 70(3).
24. Xiong, L., Xiong, N., Wang, C., Yu, X., & Shuai, M. (2019). An efficient lightweight authentication scheme with adaptive resilience of asynchronization attacks for wireless sensor networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(9), 5626-5638.
25. Yu, D., Wang, H., Chen, P. & Wei, Z. Mixed pooling for convolutional neural networks. In Rough Sets and Knowledge Technology: 9th International Conference, RSKT 2014, Shanghai, China, October 24-26, 2014, Proceedings 9, 364–375 (Springer, 2014).