Al-Qadisiyah JournalFor Engineering Sciences 18 (2025) 220 – 224

Contents lists available at: http://qu.edu.iq

Al-Qadisiyah Journal for Engineering Sciences

Journal homepage: https://qjes.qu.edu.iq

Research Paper

Optimal detection of attacks in wireless sensor networks using deep learning and Bayesian optimization

Zahraa Mehssen A. Al-Hamdawee [1], ***Humam H. Mightadh*** [1], ***and Sayyed M. Mazinani*** [2]

[1]*Department of Electrical Engineering, College of Engineering, University of Misan, Amarah 62001, Iraq.*
[2]*Department of Computer and Electrical Engineering, Imam Reza International University, Mashhad, Iran.*

ARTICLE INFO

Article history:
Received 05 December 2024
Received in revised form 15 April 2025
Accepted 22 May 2026

keyword:
Attack detection
Bayesian methods
Deep neural network
Convolutional neural network
Long short-term memory

ABSTRACT

Diagnosing attacks in wireless sensor networks (WSN) is a crucial concern in cyber security that impacts diagnosis models' accuracy because of data imbalance and outliers existence. The present paper aims to design and perform a novel strategy for efficient attack diagnosis in WSN that applies DL models' integration (DNN and CNN+LSTM) and Bayesian optimization. The present study checks concerns on data analysis such as various attack complexities and instances' imbalance. Such concerns have been mentioned by applying techniques such as MinMax scaling, data balancing with ADASYN, polynomial feature engineering, and outlier elimination with DBSCAN. The outcomes of the experiments illustrate that the DNN model obtained an F1-Score of 85.71%, and appeared an accuracy of 99.14% which is an important development across conventional techniques. Such results illustrate that was presented technique could develop WSN security and possesses high capability for various attacks' kinds' diagnosis.

1. Introduction

Attack diagnosis in WSN is known as a crucial challenge in the cyber security domain. WSNs are widely in danger of cyber threats because of their special structure and restrictions like processing capacity as well as energy use. Such attacks could ruin sensitive info and entire network performance, so, a requirement exists for improving and performing efficient techniques for such threats' identification and prevention. Here, attack diagnosis models' accuracy is impacted by issues like data imbalance and outliers [1]. One basic issue for attacks' diagnosis is data imbalance that is made by inappropriate normal and attack instances' share in a set of data. Such imbalance could cause ML models' accuracy reduction and raise false positive and false negative rates that finally cause inappropriate decisions [2]. In addition, outliers existence as unusual data could impact analysis quality negatively and result in DK models' disruption [3]. The last study illustrated that ML and DL algorithms could be efficient for attack diagnosis. For instance, Zhao et al. (2023) in a study in comparison with DL models' efficiency and classical techniques recognized that more complicated models could outperform in attack detection [4]. Additionally, Khan et al. (2023) have examined unbalanced data and outliers concerns and also improved the developed methods for accuracy improvement [5]. In the other research, Wang et al. (2024) illustrated that combined methods' usage could cause in greater outcomes rather than independent algorithms usage [6]. The present study's basic aim is to design and perform a new strategy for efficiently diagnosing attacks in WSN. Taking a lot of concerns into consideration which are present in the attack diagnosis domain, present paper checks and solves issues like attack complexity, data imbalance, and outliers. Such issues result in models' detection for reducing and providing inappropriate outcomes. To achieve the mentioned aim, DL models' integration such as LSTM, CNN, and DNN has been applied. Such integration lets the model efficiently identify complicated models in attack data. Additionally, techniques of preprocessing like outlier elimination with DBSCAN, data balancing with ADASYN, MinMax scaling, and polynomial feature engineering have been used. Such techniques straightly aid in raising model effectiveness and accuracy. Present research makes main contributions:

- Implemented advanced data preprocessing techniques including feature engineering with polynomial features and MinMax scaling to ensure better model performance.
- The utilized DBSCAN for outlier diagnosis increased the quality of data by filtering out noise points, causing a more powerful set of data.
- Applied the method of ADASYN to oversample imbalanced data, causing a well-balanced set of data. That aids in considering typical class imbalance issues in classification functions causing more reliable models.
- Leveraged Bayesian Optimization to efficiently tune hyperparameters for deep learning models (both DNN and CNN-LSTM), significantly improving model performance without exhaustive search.
- CNN with LSTM parts, efficiently getting the two spatial and temporal data attributes.

The present study's basic innovation refers to DL models' integration usage and novel pre-processing techniques that at the same time aid in solving concerns in data and developing the accuracy of identification. Especially, Bayesian optimization usage for setting optimum DL models' hyperparameters is one of the other innovations here. Such a technique lets us recognize the best hyperparameter integration for every model and extract the most optimum performance from them.

*Corresponding Authors.
E-mail address: zahraa.mo.eng@uomisan.edu.iq ; Tel: (+964) 772-829 0539 (Zahraa Al-Hamdawee) / smajidmazinani@imamreza.ac.ir ; (Sayyed Mazinani)

https://doi.org/10.30772/qjes.2024.155627.1431

Nomenclature

Ms	The minimum number of samples.	X_{max}	The max feature value in that attribute.
X	The basic feature value in that attribute.	*Greek Symbols*	
X_{min}	The min feature value in that attribute.	ε	The minimum distance between two points.

The present paper is organized into five basic units: In the second unit, the literature review as well as the study background in the attack diagnosis domain in WSN are addressed. The third unit is discussing the study method explanation. In the fourth unit, outcomes achieved from the presented model implementation are provided and compared to conventional techniques' outcomes. At last, the final unit concludes and presents recommendations for future study.

2. 2. Related works

The attack diagnosis domain in WSNs has attracted essential attention in the last few years because of rising network deployment in crucial apps like smart cities, environmental observing, and military surveillance. Investigators have recognized different methods for increasing WSN security, especially concentrating on recognizing and facing various attacks' kinds such as data manipulation, Denial of Service (DoS), and node capture. Recent DL developments encouraged investigators to explore more essential models for diagnosing attacks. Alhasan et al. (2023) provided a CNN framework launched to diagnose bad functions in WSNs [7]. Their work showed DL's ability to automatically extract related features from raw data. In addition, papers showed that multiple models, integrating various neural network frameworks, could increase the performance of diagnosis. For instance, Altunay et al. (2023) presented multiple CNN-LSTM models that efficiently obtained the two spatial and temporal models in network traffic, causing the developed accuracy and decreased false positive rates [8]. Cui et al. (2023) provide new collaborative IDS leveraging federated DL for developing software-defined vehicular network safety. By making hybrid vehicles able to learn from each other's data when keeping privacy, the system increases diagnosis fairness and resilience in contrary to different attacks, causing it to be an essential development in vehicular network safety [9]. Deng et al. (2023) present a flow topology-based graph convolutional network (GCN) for IDS in IoT networks. Such a strategy considers restricted labeled data concerns using flow topology to get dependencies between devices. The model shows greater performance to recognize bad functions in comparison with m traditional techniques, bolding its ability for IoT security apps [10]. Cao et al. (2022) improved the developed network IDS model which integrates CNN with Bidirectional Gated Recurrent Units (BiGRUs). The framework of the model efficiently gets the two spatial and temporal network traffic attributes, causing advanced diagnosis accuracy. Outcomes show considerable increment over present systems of diagnosis, presenting a powerful solution for cybersecurity [11]. Chen et al. (2022) examined multi-objective evolutionary CNN launched for IDS in fog calculation areas. Through mentioning several objectives at the same time, like the usage of sources and accuracy, the presented model derives a balance between performance and efficiency. Present paper to optimize IDS in source-limited adjustments, the critical new cloud computation nature [12]. Basati & Faghih (2021) provides the new IoT IDS using asymmetric parallel auto-encoders for developing abilities of diagnosis. The unique framework of the model increases the extraction of features and unusual diagnoses, showing its effectiveness in recognizing different models of attack. Results propose a satisfactory direction for future study in IoT security [13]. Deng & Yang (2021) provide a multiple model that integrates sparse autoencoders with the developed genetic algorithm-based backpropagation (BP) network for IDS. The new strategy optimizes feature selection and increases the performance of the model. Results show the efficiency of the model in broad intrusions' range recognition, underscoring multiple methods' ability in cybersecurity [14]. Dixit & Silakari (2021) addresses DL algorithms' apps in cybersecurity, particularly concentrating on their effectiveness for IDS. Writers analyze different models and methods, recognizing present study trends and gaps. Their perspective presents the future examinations' roadmap, focusing on adaptive learning systems significance to consider emerging cybersecurity concerns [15]. Chandre et al. (2022) present a DL model applying CNN. The presented model contains 2 stages, intrusion prevention and diagnosis. The presented model learns helpful feature representations from widely labeled data numbers and groups them. Here, CNN is applied to avoid intrusion for WSN [16]. Talukder et al. (2024) present a new IDS strategy that combines ML methods with the Synthetic Minority Oversampling Technique Tomek Link (SMOTE-TomekLink) algorithm. Such a blend synthesizes minority samples and removals Tomek links, causing to balanced set of data which considerably increases the accuracy of diagnosis in WSNs [17]. Choudhary and Pahuja (2021) offered a DL model given the CNN classifier. The offered model contains 2 steps: intrusion prevention and diagnosis. The offered model extracts effective feature representations from broad labeled data numbers before grouping them [18]. Moundounga and Satori (2023) present a Stochastic ML-Based Attack Diagnosis System for WSNs which benefits from synergy among Hidden Markov Models (HMMs) and Gaussian Mixture Models (GMMs). The presented technique applies PCA for dimensionality decrease in the WSN set of data [19].

3. Research methodology

The present paper targets developing attack diagnoses in WSN via DL model usage and Bayesian optimization. Essential concerns here contain data imbalance as well as outliers presence which robustly impact detection models' performance. Here, through applying techniques of data preprocessing as well as performing novel models like DNN and CNN+LSTM, such concerns have been solved and models' accuracy and performance have been developed.

3.1 Collecting and preparing data

Firstly, data associated with WSN attacks were extracted from the WSN-DS dataset and prepared for later analysis. Data contains different features of the network and tags of attack kind. Here, raw data was imported and the basic stages of cleaning were examined for eliminating noise and lost amounts. Labels were changed in numerical amounts applying the Label Encoding algorithm for preparing them to enter DL models.

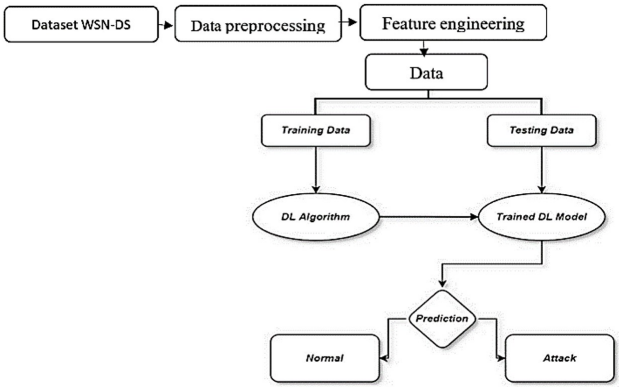

Figure 1. Proposed methodology.

3.2 Data preprocessing

To guarantee optimum models' performance, the data of input data were normalized and measured. Applying MinMaxScaler, the data were changed to a range between 0 and 1 to eliminate differences in various features' measurements. The formula for scaling is as, Eq. 1:

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \tag{1}$$

Where:
X is the basic feature value in that attribute.
X_{min} is the minimum feature value in that attribute.
X_{max} is the maximum value in that attribute.
This makes the data on a similar scale, and deep learning models can properly use it. Then, using the DBSCAN algorithm, outliers that may reduce the accuracy of the model were identified and removed. This improved the input data and prepared it better for the next steps. DBSCAN uses two main parameters:

- ε: the minimum distance between two points that can be placed in a cluster.
- $min_samples$: the minimum number of samples that must be in the neighborhood of a point to be recognized as a cluster.

This algorithm is labels that separate normal points from outliers. The points recognized as outliers are eliminated, and the present data are applied as input to learning models. The optimization formula of DBSCAN is as [20], Eq. 2.

$$DBSCAN(X.\varepsilon.min_{sample}) \tag{2}$$

That X refers to data and ε and $min_{samples}$ refer to algorithm parameters.

3.3 Feature engineering

In many complex problems, there are nonlinear relationships between features and targets (labels) that linear models alone cannot discover. For predictive model power development, we applied polynomial attributes, which let the model consider non-linear relations among attributes. The Polynomial attributes method was applied to create novel and interactive features that could aid the model in better recognizing nonlinear data models. This step was performed with the target of raising the last model's accuracy and developing the capability of detecting complex models. Polynomial features automatically make present features, Eq. 3' integrations, which contain higher degrees and attribute multiplication with each other. For example, if we have two features X_1 and X_2 in the data, the degree 2 polynomial features for these two features will be $X_1 \times X_2$ and X_{12}, X_{22}. The general formula for generating polynomial features is as follows:

$$X_{poly} = X_1 \times X_2 \ldots X_n \times X_1^2 \times X_2^2 \ldots X_n^2 \times X_1X_2 \times X_1X_3 \ldots X_{(n-1)}X_n \quad (3)$$

Where:
$X_1, X_2, \ldots, X_n$ are the main features. New features include quadratics of each feature and products between any pair of features.

3.4 Data balancing

Considering that the data were highly unbalanced and most of the samples belonged to a specific class, the ADASYN technique was used to avoid biasing the model towards frequent classes. ADASYN generates artificial samples from fewer classes to maintain data balance. This work increased the accuracy of the model and improved its performance in detecting rare but important attacks. ADASYN differs from traditional methods such as SMOTE in that ADASYN generates synthetic samples adaptively based on the local density of the minority class. That is, the harder it is to detect the boundary between classes, ADASYN generates more samples in that area to produce a better model for detecting these boundaries. ADASYN work steps are as follows [21]:
Calculation of the K-Nearest Neighbors (K-NN) distance: For each example of the minority class (attacks), its distance from other examples of the majority class is calculated and the nearest neighbors are determined. Estimation of imbalance distribution: ADASYN estimates the number of synthetic samples required for that region for each sample of the minority class. In areas where minority specimens are less abundant or harder to detect, more artificial specimens are produced.
Creation of artificial samples: New synthetic samples are generated by using the differences between the original minority samples and their nearest neighbors. These samples are added to the original data to strengthen the minority class and create more balance in the data.
Periodization of the data set: after the generation of artificial samples, new and balanced data are created and given to the learning model in the next step.

3.5 Implementing deep learning models

In stage 5, DL models' implementation was performed for attack diagnosis in WSN. This step's basic aim was to apply 2 DL models, known as CNN+LSTM and DNN for analyzing attack data and optimizing such models for obtaining the best performance. Both models were optimized by applying the Bayesian optimization technique to optimally adjust hyperparameters, such as neuron numbers in the hidden layers and rate of learning.
The first model, DNN [22], was applied as one of the broadly applied techniques in DL to extract nonlinear and complex attributes. This model includes 3 basic layers: two hidden and one input layer which applies the ReLU activation function as well as one output layer which applies the Sigmoid function for attacks' diagnosis. After designing the model, its hyperparameters were set by applying Bayesian optimization, and model training was performed by applying balanced training data and the Cross-Validation technique.
The second model, the integration of CNN+LSTM [23], was a more developed technique that applied CNN abilities for spatial feature extraction and to model temporal dependencies. Here, firstly convolutional layers were applied for spatial models' identification, and LSTM layers were applied for analyzing temporal dependencies and data continuity. Bayesian optimization was applied for setting this model hyperparameters. Outcomes illustrated that the CNN+LSTM model outperformed rather than DNN because of spatial and temporal features integration and presented greater accuracy in diagnosing attacks.
At last, after performing the two models, outcomes were compared and that was recognized that the CNN+LSTM model could obtain greater accuracy and F1 score than DNN because of its better abilities of it to analyze sequential and complicated data. To this, this model was defined as the optimum one and the proposed model here.

4. Results and discussion

4.1 Experiment setup

The experiment was performed in the Anaconda Navigator area, applying a Jupyter notebook. The presented model was performed in Python, containing various applied libraries like Seaborn, Pandas, NumPy, Scikit-learn, Keras, Matplotlib, TensorFlow, etc.

4.2 Performance evaluation metrics

To analyze our presented strategy's success, we applied various variables of performance that are determined as:
Confusion Matrix: Table 1 shows a matrix of confusion, with TP (True Positive), TN (True Negative), FP (False Positive), and FN (False Negative).

Table 1. Confusion Matrix [24].

Predicted	Actual Positive	Actual Negative
Positive	TP	FP
Negative	FN	TN

The metric of accuracy computes the appropriate rate of prediction sharing the whole accurate prediction number (TP and TN) with the entire prediction number, as illustrated in Eq. 4. Precision Eq. 5 examines the rate of accurately grouped traffic of attack for the whole forecasted traffic of attack while recall Eq. 6 shows accurately grouped attack traffic to the whole traffic of attack. F_1 score Eq. 7 is computed as the weighted precision and recall medium. ROC curves are two-dimensional charts used to assess classifier efficiency. An AUC (Area Under the Curve) score near 1 suggests high-class separation, whereas an AUC value near 0 indicates poor performance.

$$Accuracy = \frac{T_P + T_N}{T_P + T_N + F_P + F_N} \quad (4)$$

$$Precision = \frac{T_P}{T_P + F_P} \quad (5)$$

$$Recall = \frac{T_P}{T_P + F_N} \quad (6)$$

$$F_1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (7)$$

4.3 Dataset description

WSN-DS: WSN-DS was used in 2016 to recognize benign and bad transmission following nodes' numbers in WSN applying numbers. LEACH routing protocol is applied for dataset records extraction that includes 23 features. 4 various DOS attacks' kinds exist: TDMA, flooding, blackhole, and greyhole. The set includes WSN. It presents a unique insight into WSN traffic, particularly concentrating on hazards in WSNs [24].

4.4 Evaluation Results

In an analysis of multiclass outcomes, we compared different DL algorithms performance for IDS in WSN. Table 2 shows every algorithm performance score in the test. This is not valuable if higher recall, accuracy, F1 scores, and precision imply greater performance. While we compare test outcomes, we could observe that the majority of the algorithms get higher ratings of performance, showing that the method of data balancing (Adaptive Synthetic Sampling) increases total IDS performance in WSN. Table 2 illustrates different DL model's multiclass performance for IDS in WSNs such as f1-score, precision, accuracy, and recall. The comparable values of precision are 100% and 98.80%. Values of recall for such models are in turn 98.9% and 98.93%. Equal values of F1-score are 75% and 98.79%. While balancing of data was integrated into values of recall, f1-score, precision, and Adaptive Synthetic Sampling (ADASYN), accuracy was raised entirely. Between them, stably DNN showed the greatest scores of performance in whole scenarios showing that this is a model providing greater IDS performance in WSN in present condition.

Table 2. Multilabel performance analysis using Adaptive Synthetic Sampling.

DL	Accuracy	Precision	Recall	F1-score
DNN	99.14%	100%	75%	85.71%
CNN-LSTM	98.80%	98.81%	98.79%	98.8%

Figure 2 presents more info on DNN performance in comparison with other DL models in a test for IDS in WSNs. DNN has better TP and TN rates than other algorithms, illustrating a better capacity to accurately recognize the two normal intrusions and samples. DNN gets a TP rate of 33,401 TN rate of 133,704, showing that is efficient for intrusion' recognition. On the contrary, DNN has a lower rate of FP and FN, with 0 FP and 0 FN terms. Such results show the powerfulness of DNN to decrease misclassifications and develop IDS in WSN accuracy. In addition, the ROC curve in Fig. 3 illustrates the score of AUC which is the entire ML algorithms performance scale. DNN has a great AUC score of 99.99%, showing its proficiency in recognizing intrusions. A high AUC score illustrates that DNN possesses a high TP ratio when maintaining a low FP ratio, causing that to be a great candidate for IDS in WSNs.

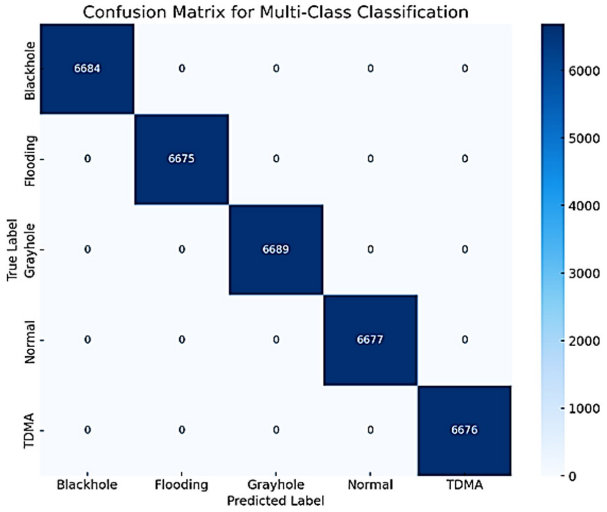

Figure 2. Confusion matrix for multiclass in DNN.

Our model performed better than standard strategies in various parameters of performance after situational research and comparison. The capability for intrusions' detection, decreasing false favorable ratios also control of imbalanced sets of data distinguishes it as the best response for IDS in WSNs. Companies and investigators could take advantage of our model's powerful and trustworthy IDS algorithm that develops whole WSNs security conditions and also allows for simple implementation in various adjustments of real life.

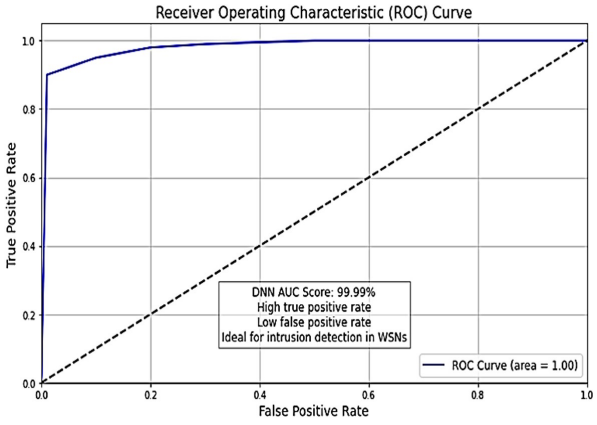

Figure 3. ROC Curve for multiclass classification.

Table 3 compares various WSN IDS for WSN-DS. Such models apply different methods and algorithms for recognizing intrusions, also their performance is scaled by applying ratios of accuracy. This discussion will concentrate on our proposal's performance in multiclass conditions and approaches applied in our pinnacles. In the WSN IDS domain, different prominent papers apply various methods and mechanisms. For instance, [18] applies CNN for multiclass IDS, getting a 97% ratio of accuracy. [19] applied Hidden Markov Models (HMMs) and Gaussian Mixture Models (GMMs) in multiclass diagnosis, getting an accuracy of 94.55%. Our proposal accurately performs better than the last study in multiclass IDS scenarios. In multiclass diagnosis, our 99.14% accuracy rate performs better than other models.

Table 3. Comparison analysis of wireless sensor intrusion detection models in WSN-DS.

NO.	Data balancing technique	Algorithm	Dataset	Class	Accuracy rate (%)
[18]	Not specified	CNN	WSN DS	Flooding, Blackhole, etc.	97.00%
[19]	SMOTE	HMMs and GMMs	WSN DS	Various (including Flooding)	94.55%
Proposed method	ADASYN	DNN and CNN+LSTM	WSN DS	TDMA, flooding, blackhole, greyhole	99.14%

In this study, our suggested solution, which combines the ADASYN data balancing technique with the DNN and CNN+LSTM deep learning models, improved classification accuracy by 99.14%. These findings are significantly superior to prior methods such as the CNN model without data balancing [18] and HMMs and GMMs utilizing the SMOTE technique, [19]. For example, despite a respectable accuracy of 97%, the approach [18] may suffer from class imbalance because to a lack of data balancing techniques. Furthermore, the approach [19], which employs SMOTE to balance data and statistical models, has achieved an accuracy of 94.55The time complexity of the proposed deep learning models was also investigated. The CNN model, with time complexity $O(F \times K2 \times W \times H)$, is effective in detecting attacks due to its ability to learn spatial patterns. F: the number of filters (kernels) in the convolution layer, $K2$: filter size (kernel size), W and H: width and height of the feature map output after applying the convolution operation. Adding LSTM to the CNN model improved temporal pattern learning, but increased the time complexity to $O(H2 \times T)$.
H: the number of hidden units in the LSTM layer. T: sequence length. Combining these models with DNN to extract non-spatial information yielded a powerful framework with excellent classification capabilities. In terms of data balancing strategies, ADASYN has been able to generate more synthetic data for difficult classes while also improving class balance. This strategy substantially boosted the model's capability in detecting attacks by focusing on samples that are naturally difficult to classify. ADASYN has a larger computing cost than SMOTE ($O(Nminoority \times P)$. Nminority: the number of examples in the minority class. P: the number of features (dimensions or features) of the data, but the results justify the complexity. It should be mentioned that all of the experiments in this study were conducted on NVIDIA Tesla V100 GPU hardware with 16 GB RAM. The proposed model's training execution time, which included data balancing, feature learning, and classification, was reported at approximately X minutes on average. Given the excellent accuracy of 99.14%, this computational cost is acceptable as a positive point for real-world applications. This investigation demonstrates that the use of modern data balancing techniques and deep learning models, combined with appropriate hardware, may effectively address the issues of wireless sensor network data classification.

5. Conclusion

The present article increasingly develops assault diagnosis in WSNs by applying DL models and Bayesian optimization methods. This study efficiently controlled normal data imbalance and outliers challenge that frequently restrict model performance, applying systematic techniques that encompassed data balancing, gathering, feature engineering, and preprocessing. The method considerably improved accuracy and diagnosis abilities using developed models like DNN and CNN combined with CNN+LSTM. ADASYN method usage for data balance and the DBSCAN algorithm for outlier removal were crucial to developing input data quality, causing more reliable predictions. In addition, the strategy of SHAP presented effective perspectives on feature significance that developed the model's transparency and interpretability. Future research can consider applying ensemble learning techniques for developing diagnosis accuracy and powerfulness in contrast to different kinds of attacks in WSNs. Also, examining real-life data flows for ongoing model adaption might raise solutions to present threats.

Authors' contribution

All authors contributed equally to the preparation of this article.

Declaration of competing interest

The authors declare no conflicts of interest.

Funding source

This study didn't receive any specific funds.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with ai and machine learning methods," *Journal of Big Data*, vol. 11, no. 1, p. 16, 2024. [Online]. Available: https://doi.org/10.1186/s40537-023-00870-w

[2] E. A. Al-Qarni and G. A. Al-Asmari, "Addressing imbalanced data in network intrusion detection: A review and survey," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 15, no. 2, pp. 000–000, 2024. [Online]. Available: https://dx.doi.org/10.14569/IJACSA.2024.0150215

[3] L. Zolfagharipour, M. H. Kadhim, and T. H. Mandeel, "Enhance the security of access to iot-based equipment in fog," vol. 00, no. 00, 2023, pp. 142–146. [Online]. Available: https://doi.org/10.1109/AICCIT57614.2023.10218280

[4] F. Zhao, H. Li, K. Niu, J. Shi, and R. Song, "Application of deep learning-based intrusion detection system (ids) in network anomaly traffic detection," *Applied and Computational Engineering*, vol. 86, no. 00, pp. 231–237, 2024. [Online]. Available: https://doi.org/10.54254/2755-2721/86/20241604

[5] A. A. Khan, O. Chaudhari, and R. Chandra, "A review of ensemble learning and data augmentation models for class imbalanced problems: Combination, implementation and evaluation," *Expert Systems with Applications*, vol. 244, no. 00, p. 122778, 2024. [Online]. Available: https://doi.org/10.1016/j.eswa.2023.122778

[6] Z. Wang, Y. Liu, D. He, and S. Chan, "Intrusion detection methods based on integrated deep learning model," *Computers & Security*, vol. 103, no. 00, p. 102177, 2021. [Online]. Available: https://doi.org/10.1016/j.cose.2021.102177

[7] R. A. Alhasan and E. K. Hamza, "A novel cnn model with dimensionality reduction for wsn intrusion detection," *Revue d'Intelligence Artificielle*, vol. 37, no. 5, pp. 1121–1131, 2023. [Online]. Available: https://doi.org/10.18280/ria.370504

[8] H. C. Altunay and Z. Albayrak, "A hybrid cnn+lstm-based intrusion detection system for industrial iot networks," *Engineering Science and Technology, an International Journal*, vol. 38, no. 00, p. 101322, 2023. [Online]. Available: https://doi.org/10.1016/j.jestch.2022.101322

[9] J. Cui *et al.*, "Collaborative intrusion detection system for sdvn: A fairness federated deep learning approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 9, pp. 2512–2528, 2023. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/TPDS.2023.3290650

[10] X. Deng, J. Zhu, X. Pei, L. Zhang, Z. Ling, and K. Xue, "Flow topology-based graph convolutional network for intrusion detection in label-limited iot networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 684–696, 2023. [Online]. Available: https://doi.org/10.1109/TNSM.2022.3213807

[11] B. Cao, C. Li, Y. Song, and X. Fan, "Network intrusion detection technology based on convolutional neural network and bigru," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, p. 1942847, 2022. [Online]. Available: https://doi.org/10.1155/2022/1942847

[12] Y. Chen, Q. Lin, W. Wei, J. Ji, K.-C. Wong, and C. A. C. Coello, "Intrusion detection using multi-objective evolutionary convolutional neural network for internet of things in fog computing," *Knowledge-Based Systems*, vol. 244, no. 00, p. 108505, 2022. [Online]. Available: https://doi.org/10.1016/j.knosys.2022.108505

[13] A. Basati and M. M. Faghih, "Apae: an iot intrusion detection system using asymmetric parallel auto-encoder," *Neural Computing and Applications*, vol. 35, no. 7, pp. 4813–4833, 2023. [Online]. Available: https://doi.org/10.1007/s00521-021-06011-9

[14] H. Deng and T. Yang, "Network intrusion detection based on sparse autoencoder and iga-bp network," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, p. 9510858, 2021. [Online]. Available: https://doi.org/10.1155/2021/9510858

[15] P. Dixit and S. Silakari, "Deep learning algorithms for cybersecurity applications: A technological and status review," *Computer Science Review*, vol. 39, no. 00, p. 100317, 2021. [Online]. Available: https://doi.org/10.1016/j.cosrev.2020.100317

[16] P. Chandre, P. Mahalle, and G. Shinde, "Intrusion prevention system using convolutional neural network for wireless sensor network," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 11, no. 2, pp. 504–515, 2022. [Online]. Available: http://doi.org/10.11591/ijai.v11.i2.pp504-515

[17] M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, "Mlstl-wsn: machine learning-based intrusion detection using smotetomek in wsns," *International Journal of Information Security*, vol. 23, no. 3, pp. 2139–2158, 2024. [Online]. Available: https://doi.org/10.1007/s10207-024-00833-z

[18] D. Choudhary and R. Pahuja, "Prevention of intrusion attacks via deep learning algorithm in wireless sensor network in smart cities," in *Advances in Clean Energy Technologies*, ser. Springer Proceedings in Energy, P. V. Baredar, S. Tangellapalli, and C. S. Solanki, Eds. Springer Singapore, 2021, pp. 501–521. [Online]. Available: https://doi.org/10.1007/978-981-16-0235-1_40

[19] A. R. A. Moundounga and H. Satori, "Stochastic machine learning based attacks detection system in wireless sensor networks," *Journal of Network and Systems Management*, vol. 32, no. 1, p. 17, 2023. [Online]. Available: https://doi.org/10.1007/s10922-023-09794-5

[20] Y. Yang *et al.*, "An efficient dbscan optimized by arithmetic optimization algorithm with opposition-based learning," *The Journal of Supercomputing*, vol. 78, no. 18, pp. 19 566–19 604, 2022. [Online]. Available: https://doi.org/10.1007/s11227-022-04634-w

[21] J. Brandt and E. Lanzén, "A comparative review of smote and adasyn in imbalanced data classification," Uppsala University, Tech. Rep., 2021, bSc Research. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-432162

[22] V. Gowdhaman and R. Dhanapal, "An intrusion detection system for wireless sensor networks using deep neural network," *Soft Computing*, vol. 26, no. 23, pp. 13 059–13 067, 2022. [Online]. Available: https://doi.org/10.1007/s00500-021-06473-y

[23] S. Salim and L. Oughdir, "Cnn-lstm based approach for dos attacks detection in wireless sensor networks," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 4, pp. 835–842, 2022. [Online]. Available: https://dx.doi.org/10.14569/IJACSA.2022.0130497

[24] I. Almomani, B. Al-Kasasbeh, and M. AL-Akhras, "Wsn-ds: A dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, vol. 2016, no. 1, p. 4731953, 2016. [Online]. Available: https://doi.org/10.1155/2016/4731953

How to cite this article:
Zahraa Mehssen A. Al-Hamdawee, Humam H. Mightadh and Sayyed M. Mazinani. (2026). 'Optimal detection of attacks in wireless sensor networks using deep learning and Bayesian optimization', Al-Qadisiyah Journal for Engineering Sciences, 19 (2), pp. 220-224. https://doi.org/10.30772/qjes.2024.155627.1431