Resource-Aware CNN-IIDS for Intrusion Detection in WSNs with Multi-Dataset Evaluation

Sumedh Dhengre
Department of Computer Engineering, AISSMS College of Engineering, Savitribai Phule Pune University, Pune, India
sumedhdhengre@gmail.com (corresponding author)

Shabnam Sayyad
Department of Computer Engineering, AISSMS College of Engineering, Savitribai Phule Pune University, Pune, India
ssshaikh@aissmscoe.com

Received: 16 April 2026 | Revised: 6 May 2026, 21 May 2026, and 23 May 2026 | Accepted: 24 May 2026

 DOI: https://doi.org/10.48084/etasr.19346

ABSTRACT

Wireless Sensor Networks (WSNs) are vulnerable to cyber-attacks due to their limited energy and computational resources. This study proposes a resource-aware Convolutional Neural Network-based Intelligent Intrusion Detection System (CNN-IIDS) for efficient multi-attack detection in WSN environments. The framework integrates hybrid feature engineering, combining traffic-based features with node-level resource metrics. The framework employs a lightweight CNN for automated feature learning and classification. The proposed system detects multiple attacks, including Denial of Service (DoS), User-to-Root (U2R), Remote-to-Local (R2L), and Wormhole attacks. To ensure robustness, the model is evaluated on multiple datasets, including simulation-based and benchmark datasets such as WSN-DS, and is compared with machine learning classifiers, including Random Forest. The experimental results demonstrate high detection accuracy, precision, recall, and low false positive rates. The proposed CNN-IIDS achieves an effective balance between performance and computational efficiency, making it suitable for resource-constrained WSN environments.

Keywords-Wireless Sensor Networks (WSNs); Intrusion Detection System (IDS); Convolutional Neural Network (CNN); resource-aware model; multi-attack detection; multi-dataset evaluation; network security

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of distributed, self-organizing sensor nodes that communicate wirelessly without centralized infrastructure. WSNs are widely used in applications such as environmental monitoring, healthcare, and military systems. However, due to their open deployment, dynamic topology, and limited energy and computational resources, WSNs are highly vulnerable to various security threats, including Denial of Service (DoS), routing attacks, and node compromise [1, 7, 8]. Traditional security mechanisms such as encryption and authentication are often insufficient in such constrained environments [9-12]. Intrusion Detection Systems (IDSs), therefore, play a crucial role in improving network security by monitoring traffic behavior and detecting malicious activities [2, 3]. IDS techniques are broadly categorized into signature-based and anomaly-based methods. While signature-based approaches are efficient for known attacks, they fail to detect unknown threats, whereas anomaly-based approaches offer better adaptability for dynamic WSN environments [13-16]. Advancements emphasize machine learning-based IDS models due to their ability to improve detection accuracy, adaptability, and scalability [4-6].

Early IDS approaches based on rule-based, statistical, and supervised machine learning techniques provided efficient detection of known attacks with relatively low computational overhead. However, these approaches demonstrated limited capability in identifying unknown and sophisticated attack patterns in dynamic WSN environments [11, 17-20]. To overcome these limitations, research introduced hybrid, ensemble, and deep learning-based IDS models incorporating techniques such as SMOTE, PCA, Convolutional Neural Network (CNN), and attention mechanisms for improved feature extraction and multi-attack detection [21-23, 25, 29]. Although these approaches achieved higher detection accuracy and lower false positive rates, they often increased computational complexity, energy consumption, and deployment overhead. These factors limit their suitability for resource-constrained WSN environments. Furthermore,

federated learning and explainable AI-based IDS approaches improved privacy preservation and model interpretability but still face communication overhead and deployment challenges in distributed sensor networks [24, 26-28].

Lightweight, intelligent, and energy-aware security mechanisms for WSN and IoT environments have been investigated. Authors in [30, 32] proposed secure and energy-efficient routing protocols for resource-constrained sensor networks to improve network lifetime and secure communication efficiency. Authors in [31] utilized data analytics for malicious insider attack detection in IoT systems, demonstrating the effectiveness of intelligent anomaly detection techniques in identifying abnormal network behavior. Blockchain-based and AI-driven security frameworks have been explored to enhance distributed cybersecurity architectures and intelligent decision-making capabilities [33, 34]. The present study proposes a CNN-IIDS, which focuses on lightweight and resource-aware multi-attack intrusion detection in hierarchical WSN environments. The framework employs deep learning-based traffic analysis at cluster heads and centralized IDS units. A comparative summary of the existing approaches, along with their strengths and limitations, is presented in Table I.

TABLE I. COMPARATIVE ANALYSIS OF EXISTING IDS APPROACHES IN WSNS

Reference	Method used	Advantages	Limitations
[19, 20]	Support Vector Machine (SVM)-based IDS	High accuracy	Poor unknown attack detection
[4, 21]	SMOTE, PCA	Improved classification	Increased complexity
[22, 23]	CNN/deep learning	Multi-attack detection	High computation overhead
[24, 27]	Federated learning	Privacy preservation	Communication overhead
[26, 28]	Explainable AI	Energy-efficient, interpretable	Additional processing cost
[30, 32]	Secure routing protocols	Energy-aware secure communication	Limited IDS functionality
[31]	Data analytics IDS	Insider attack detection	Limited deep learning capability
[33]	Blockchain security	Distributed trust management	Not WSN IDS-specific
[34]	AI pattern recognition	Intelligent classification	Not intrusion-focused

Despite significant advancements, existing IDS models often prioritize detection accuracy while overlooking false alarm reduction, robustness, scalability, and resource efficiency in real-world WSN environments. Many approaches are evaluated on limited attack scenarios and introduce high computational overhead, making them unsuitable for energy-constrained sensor networks [26-29]. Therefore, there is a need for a lightweight and scalable IDS capable of accurate multi-attack detection with optimized resource utilization. To address these challenges, the proposed resource-aware CNN-IIDS targets DoS, User-to-Root (U2R), Remote-to-Local (R2L), and Wormhole attacks within a unified framework. The model emphasizes lightweight architecture, optimized feature handling, and efficient preprocessing to improve detection accuracy while minimizing computational overhead. Evaluation using the WSN-DS dataset under multi-attack scenarios further ensures realistic performance assessment and practical applicability in hierarchical WSN environments.

II. INTELLIGENT INTRUSION DETECTION SYSTEM(IIDS)

The proposed resource-aware CNN-IIDS is designed to detect multiple attacks in WSNs while considering resource constraints such as limited energy and computational capacity. As illustrated in Figure 1, the system begins with network traffic acquisition using NS-2-based simulations, ensuring representation of both normal and malicious activities. The collected data include packet-level attributes, such as transmission rate, delay, and packet size, and node-level characteristics, including energy consumption, neighbor interactions, and routing behavior. The collected data capture both communication patterns and resource dynamics. The raw data are preprocessed using noise removal, normalization, encoding, and feature scaling to ensure consistency and reduce computational overhead.

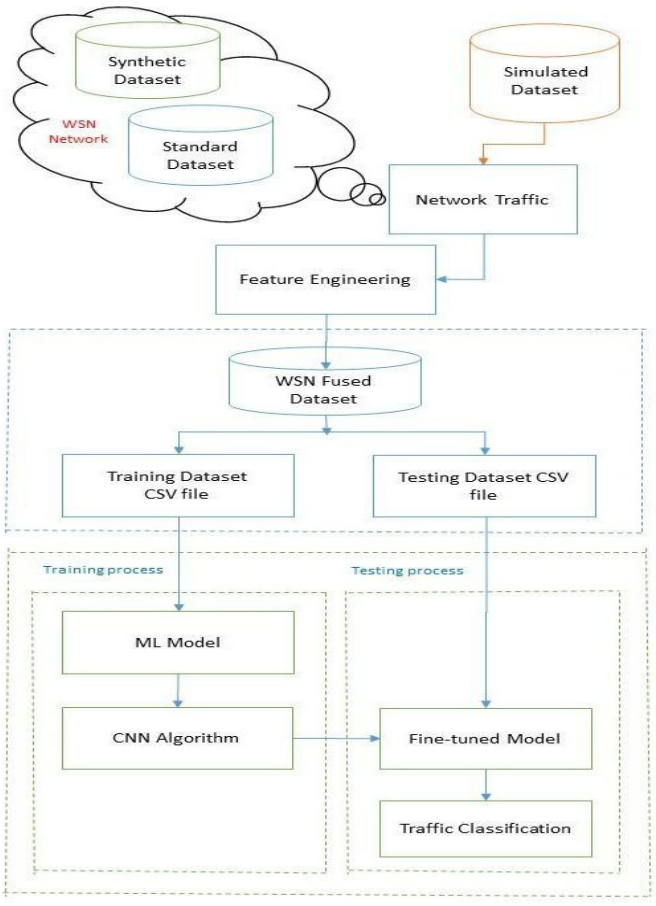

Fig. 1. Proposed IIDS architecture for adaptive WSN security.

To effectively represent intrusion behavior, a hybrid feature engineering strategy is adopted by combining traffic-based

features (e.g., packet rate, drop ratio, routing consistency) with resource-aware node metrics (e.g., energy consumption trends and communication density). The processed features are then input into a lightweight CNN, which serves as the core component of the proposed CNN-IIDS. The CNN performs automated feature learning and captures hidden spatial and non-linear relationships in network traffic, enabling improved detection of complex and multi-attack patterns. This approach reduces dependency on manual feature selection. It simultaneously enhances the model's ability to generalize across diverse attack scenarios while maintaining efficiency suitable for WSN environments. To validate the effectiveness of the CNN-based model, multiple machine learning algorithms, including Logistic Regression, Decision Trees, SVM, Naïve Bayes, Random Forest, and XGBoost, are evaluated as baseline models. Among these, Random Forest demonstrates strong performance and is used as a benchmark for comparative analysis, instead of the primary model. The dataset is divided into training (80%), validation (10%), and testing (10%) sets. The model performance is evaluated using metrics such as accuracy, precision, recall, F1-score, and the false positive rate. The results show that the CNN-based approach achieves improved detection capability for multiple attacks, including DoS, U2R, R2L, and Wormhole attacks, while maintaining a balance between accuracy and computational efficiency, making it suitable for resource-constrained WSN environments.

III. SIMULATION AND DATASETS ANALYSIS

A. *Simulation Environment*

Simulations were performed using the NS-2 simulator to evaluate the proposed multi-attack detection model in WSNs. A total of 50 sensor nodes were randomly deployed over a 1024 cm × 768 cm area, representing a moderate WSN scenario, as depicted in Table II.

TABLE II. SIMULATION PARAMETERS

Parameter	Value
Routing protocol	AODV
MAC layer protocol	802.11
Total number of nodes	50
Traffic type	Constant Bit Rate (CBR)
Simulation topology	1024 cm × 768 cm
Simulation time	100 sec
Packet size	512 Kbytes

The network was configured using the AODV routing protocol and the IEEE 802.11 MAC layer to ensure realistic communication behavior. The simulation was executed for 100 s with the Constant Bit Rate (CBR) traffic and a packet size of 512 bytes, generating a consistent network load. The WSN environment was further modeled by configuring parameters such as node density, network area, and transmission range. Nodes are deployed and visually distinguished, with initial communication established through Hello packet broadcasting, as displayed in Figure 2. The network operates under both normal and adversarial conditions, where malicious nodes inject forged packets to disrupt standard communication patterns. All network activities were recorded in a trace file (trace.txt), which serves as input to the proposed IDS.

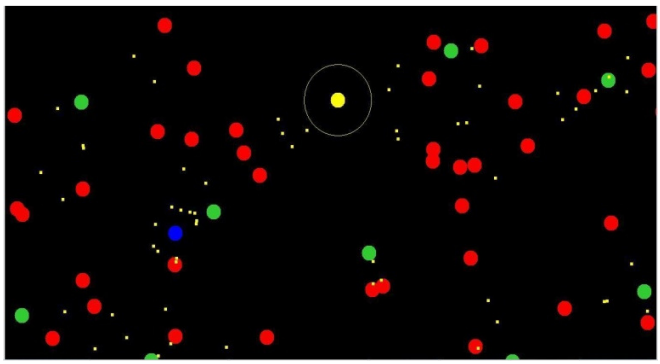

Fig. 2. Attack simulation in WSN using NS-2.

B. *Dataset Analysis*

Three datasets were used for evaluation: the Simulation Dataset (50,452 records) generated from NS-2 trace files, the Synthesized Dataset (2,000 records) representing rare attack patterns, and the standard WSN-DS Dataset [4] (374,661 records) for large-scale validation. Each dataset was individually preprocessed through noise removal, normalization, encoding, and feature extraction to ensure consistency. A unified feature space was created by aligning common attributes and removing redundant or non-overlapping features, followed by record-level merging and label harmonization. To prevent bias due to dataset imbalance, class-balancing techniques were applied. The final dataset was shuffled and split into training, validation, and testing sets. The Synthesized Dataset includes 14 attributes capturing node- and packet-level behavior under normal and attack conditions, such as Timestamp, Node_ID, Packet_Type, Packet_Size, RSSI, Delay, Hop_Count, TTL, Flags, Packet_Payload, Packet_Priority, and Attack_Type, as presented in Table III.

TABLE III. SELECTED FEATURES AND THEIR RELEVANCE FOR MACHINE LEARNING-BASED IDS IN WSNS

Feature	Type	Reason for selection
Packet_Type	Categorical	Distinguishes control and data packets; anomalies observed in DoS and Wormhole attacks.
Packet_Size	Numerical	Abnormal packet sizes indicate flooding behavior in DoS attacks.
Packet_RSSI	Numerical	Irregular signal strength helps detect spoofing and Wormhole attacks.
Packet_Delay	Numerical	Increased delay is a strong indicator of DoS and network congestion.
Packet_Priority	Categorical	Unusual hop counts reveal routing anomalies in Wormhole attacks.
Packet_Hop_Count	Numerical	Abnormal TTL values indicate packet manipulation and flooding attacks.
Packet_TTL	Numerical	Identifies suspicious connection patterns in U2R and R2L attacks.
Packet_Flags	Categorical	Detects hidden or malicious payload patterns in U2R and R2L attacks.

The proposed system employs a CNN for automated feature extraction and multi-attack detection, eliminating manual feature engineering. The model was trained using cross-

validation to ensure generalization, and was evaluated using accuracy, precision, recall, F1-score, and the false positive rate to assess effectiveness, robustness, and efficiency. To enhance detection accuracy, a subset of these features was selected for machine learning models, focusing on both traffic-based and derived metrics such as Payload Entropy, which assists in identifying encrypted or malicious payloads. Selected features encompass categorical variables (Packet_Type, Packet_Priority, Packet_Flags) and numerical indicators (Packet_Size, Packet_RSSI, Packet_Delay, Packet_Hop_Count, Packet_TTL) that effectively capture anomalies introduced by DoS, spoofing, and flooding attacks.

IV. EXPERIMENTATION SETUP AND STRATEGY ANALYSIS

A. Experimentation Setup

The model was implemented using TensorFlow and evaluated using NS-2 simulations along with benchmark datasets, including WSN-DS. Multiple attack types, such as DoS, U2R, R2L, and Wormhole attacks, were considered. The datasets were preprocessed using normalization and feature alignment, followed by merging into a unified dataset with class balancing through resampling. The CNN architecture includes two convolutional layers (32 and 64 filters), max-pooling, and a dense layer, trained using the Adam optimizer (learning rate 0.001, batch size 64, 50 epochs). Using 5-fold cross-validation, the model achieved an average accuracy of 92.8% (±1.4) with consistent precision, recall, and F1-score.

B. Machine Learning Algorithmic Strategy Analysis

The proposed CNN-IIDS adopts a hybrid machine learning framework for multi-attack detection and real-time intrusion analysis in resource-constrained WSNs. A lightweight CNN with only two convolutional layers (32 and 64 filters) serves as the primary detection model, while Logistic Regression, Decision Tree, SVM, Naïve Bayes, Random Forest, and XGBoost are utilized for comparative evaluation and benchmarking. The shallow CNN architecture significantly reduces computational complexity, trainable parameters, FLOPs, memory consumption, and training overhead compared to deeper CNN models while maintaining effective detection of complex attack patterns through automatic feature extraction and deep representation learning.

The developed model has a compact size of approximately 5.6 MB, making it suitable for practical hierarchical WSN deployments. Although typical sensor motes may have less than 256 kB of RAM, the proposed CNN-IIDS is primarily intended for deployment at resource-capable cluster heads and centralized IDS units rather than highly constrained sensing nodes.

Fig. 3. Intrusion detection graph for a DoS attack.

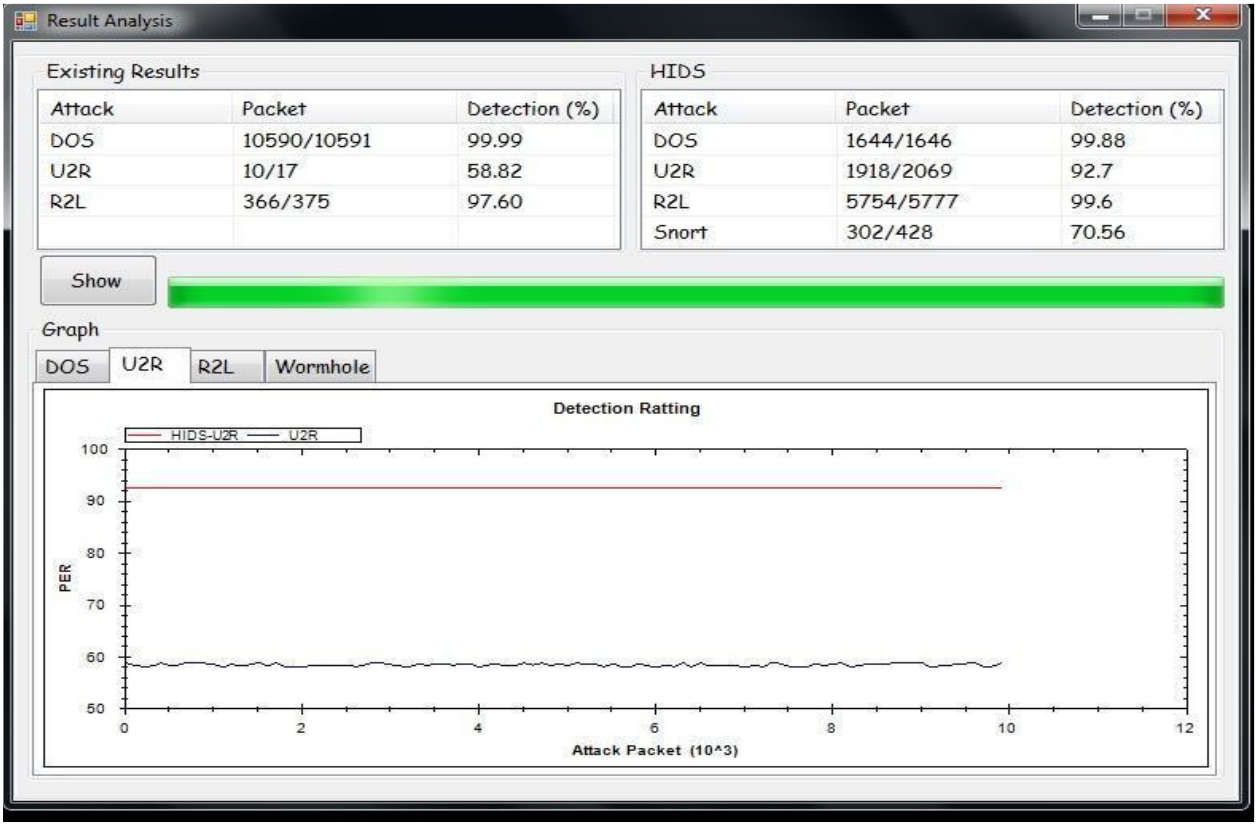

Fig. 4. Intrusion detection graph for a U2R attack.

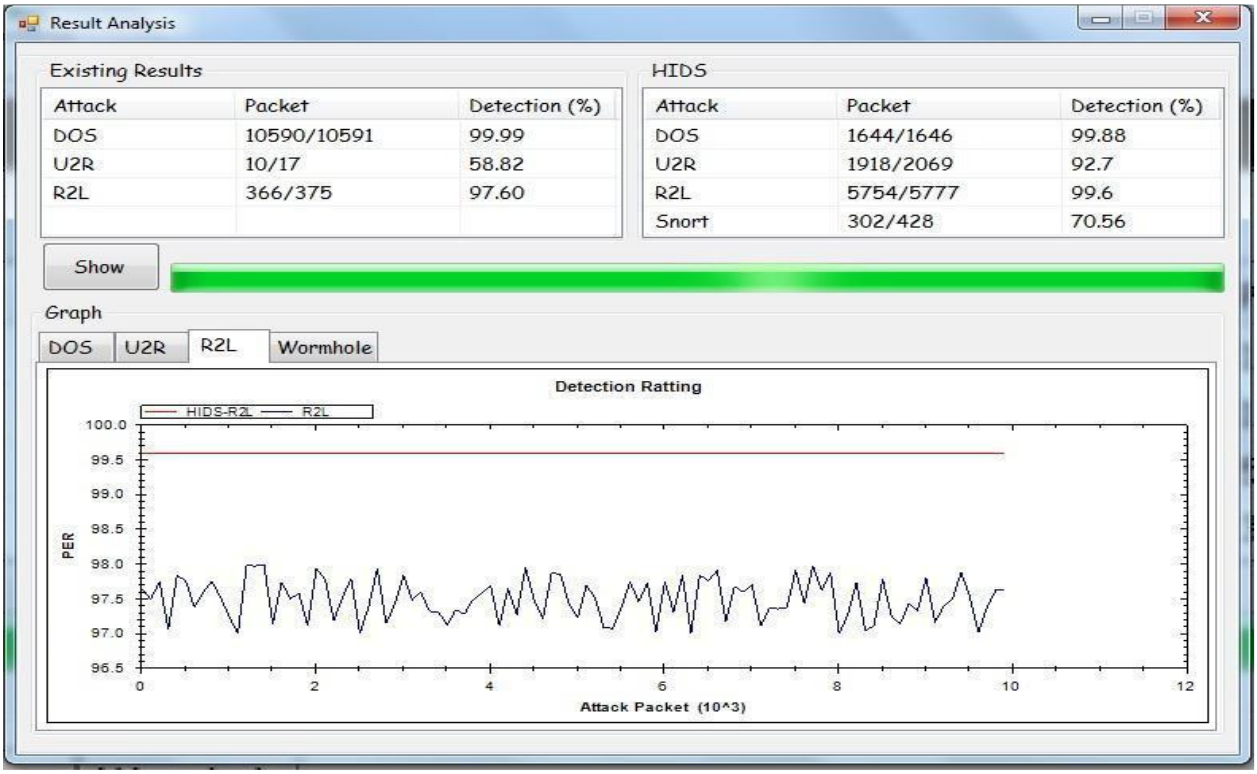

Fig. 5. Intrusion detection graph for an R2L attack.

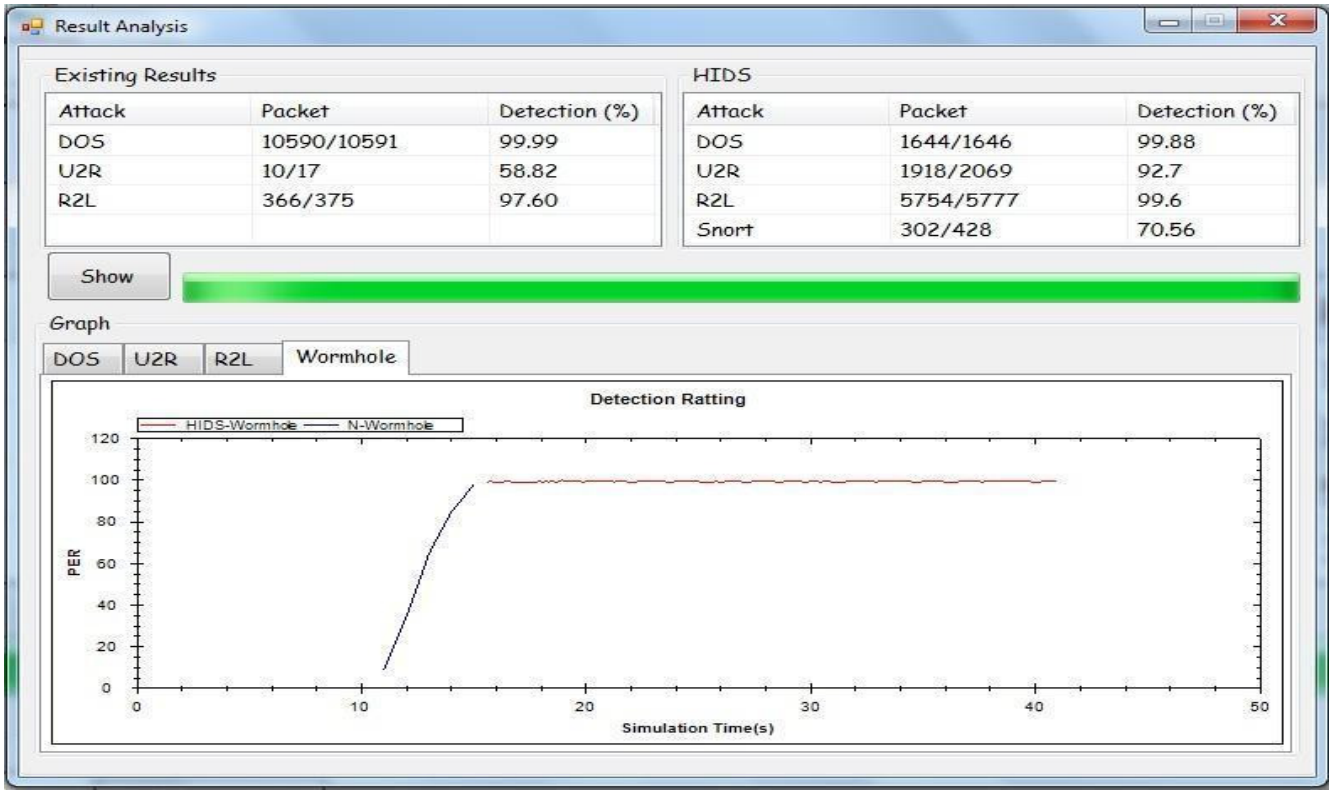

Fig. 6. Intrusion detection graph for a Wormhole attack.

The threat model considers both external attackers and compromised internal nodes capable of launching DoS, U2R, R2L, and Wormhole attacks, including scenarios involving multiple malicious nodes and attacks that partially mimic legitimate traffic behavior. In hierarchical WSN environments, intrusion detection tasks are commonly offloaded to cluster heads or centralized monitoring systems to minimize computational burden and energy consumption at sensor nodes. Overall, the proposed CNN-IIDS achieves a balance between detection accuracy, computational efficiency, and practical deployability for real-world WSN security applications.

V. RESULTS AND COMPARATIVE ANALYSIS

A. Results and Discussions

The proposed CNN-based model effectively distinguishes between normal and malicious traffic, enabling accurate detection of multiple attacks, including DoS, U2R, R2L, and Wormhole. The IDS output, as illustrated in Figure 3, presents key performance indicators, such as detection accuracy and predicted attack classes, while also identifying malicious nodes for isolation through the Base Station. Figures 3-6 further demonstrate detection behavior across various attack scenarios.

A detailed detection window provides information on the attack type, applied rules, and attacker attributes, supporting efficient monitoring and analysis. The proposed CNN-IIDS achieves an overall detection accuracy of 92.8% (±1.4), with consistent precision (91.9%), recall (92.3%), and F1-score (92.1%), indicating stable performance across different conditions. The confusion matrix and per-class performance analysis portrayed in Figure 7 and Table IV demonstrate the effectiveness of the proposed model for multi-attack detection in hierarchical WSN environments.

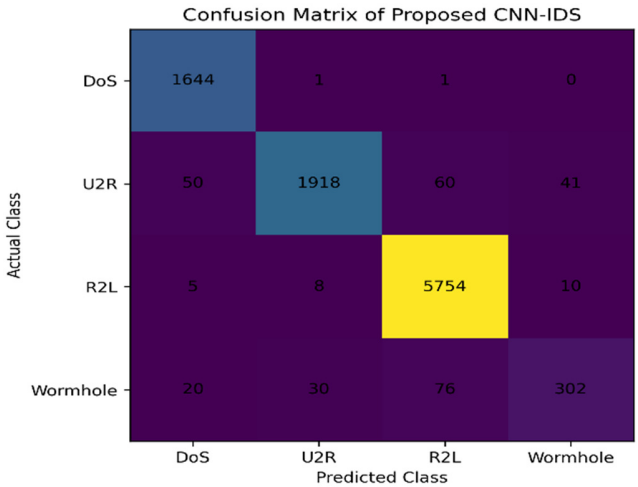

Fig. 7. Confusion matrix of the proposed CNN-based IDS.

The majority of instances are correctly classified, with only minor misclassifications observed between certain attacks and normal traffic. The model achieves comparatively higher precision and recall for DoS and R2L attacks due to their distinct abnormal traffic characteristics and communication patterns. In contrast, minor misclassifications are observed in

U2R and Wormhole attacks because such attacks often generate subtle behavioral variations and partially resemble legitimate network traffic, making classification more challenging. Furthermore, ROC analysis indicates AUC values above 0.90 for all classes, confirming the strong discriminative capability, generalization performance, and reliability of the proposed IDS in resource-aware WSN architectures.

TABLE IV. ATTACK-WISE PERFORMANCE ANALYSIS

Attack type	Precision (%)	Recall (%)	F1-score (%)
DoS	95.64	99.88	97.71
U2R	98.01	92.70	95.28
R2L	97.67	99.60	98.63
Wormhole	85.55	70.56	77.34

B. Comparative Analysis

Comparative analysis with existing intrusion detection techniques is performed using detection rate as the primary metric. The results presented using the proposed approach achieve superior performance, as indicated by the higher detection rate curve, along with reduced energy consumption and low latency. While the detection rate for DoS remains comparable to previous work, significant improvements of approximately 33% and 2% are observed for U2R and R2L attacks, respectively. Additionally, the model maintains low false positive rates and an average inference time of approximately 3.2 ms per sample, confirming its efficiency for real-time deployment. Overall, these results highlight that the proposed model outperforms existing techniques in terms of detection accuracy, computational efficiency, and reliability for multi-attack detection in WSN environments.

To validate the claims of low energy consumption, low latency, and efficiency, additional performance metrics were evaluated, as exhibited in Table V. The proposed CNN-based IDS achieved a low inference time of 3.2 ms per sample, a reduced energy consumption of 0.65 mJ, a moderate memory usage of 120 MB, and a compact model size of 5.6 MB, demonstrating suitability for resource-aware WSN environments. The model achieved an improved detection rate of 95.25% while reducing false positives from 6% to 2.75% compared to traditional IDS approaches such as SVM, KNN, and Decision Tree. Furthermore, the computational complexity analysis confirmed efficient scalability with input size, while lower latency and faster response time validated the effectiveness of the proposed IDS for real-world hierarchical WSN deployments.

TABLE V. ENERGY AND LATENCY PERFORMANCE COMPARISON OF IDS MODELS

Model	Detection rate (%)	False positive rate (%)	Inference time (ms)	Energy consumption (mJ)	Memory usage (MB)
SVM	88.0	6.0	5.8	0.95	140
KNN	84.2	7.2	6.5	1.10	160
Decision Tree	82.8	7.8	4.9	0.85	110
Proposed CNN	95.25	2.75	3.2	0.65	120

VI. CONCLUSION

Wireless Sensor Networks (WSNs) are vulnerable to multiple security threats due to their distributed architecture and resource-constrained nature. Existing Intrusion Detection System (IDS) approaches often focus mainly on detection accuracy while overlooking computational overhead, false alarms, scalability, and real-time deployment feasibility in multi-attack environments. To address these limitations, the present study proposed a lightweight and resource-aware Convolutional Neural Network-based Intelligent Intrusion Detection System (CNN-IIDS) framework for multi-attack detection in hierarchical WSN architectures.

The proposed framework utilizes a shallow CNN architecture with two convolutional layers (32 and 64 filters), enabling reduced computational complexity, trainable parameters, FLOPs, memory usage, and training overhead while maintaining effective detection capability. The framework successfully detects Denial of Service (DoS), User-to-Root (U2R), Remote-to-Local (R2L), and Wormhole attacks using optimized preprocessing and deep feature extraction techniques. Experimental evaluation employing the WSN-DS dataset achieved an overall detection accuracy of 92.8% (±1.4), with precision, recall, and F1-score values of 91.9%, 92.3%, and 92.1%, respectively. The proposed model also improved the detection rate from 88% to 95.25% while reducing false positives from 6% to 2.75% compared to traditional IDS approaches such as SVM, KNN, and Decision Tree. Furthermore, the model demonstrated low inference time (3.2 ms), reduced energy consumption (0.65 mJ), moderate memory usage (120 MB), and a compact model size of 5.6 MB, confirming its suitability for resource-aware hierarchical WSN deployments.

Overall, the proposed CNN-IIDS provides an efficient and scalable framework for real-time intrusion detection with improved adaptability, reduced computational overhead, and practical deployability compared to existing approaches. Future work will focus on integrating federated learning, explainable AI techniques, and real-world large-scale WSN deployment validation to further enhance security, interpretability, and ultra-low-power edge deployment capability.

DECLARATION OF COMPETING INTERESTS

The authors declare no competing interests.

ACKNOWLEDGMENT

The authors express their sincere gratitude to Dr. Shabnam Sayyad for her valuable guidance and continuous support. The authors also acknowledge AISSMS' COE, Pune, as the research center for providing the necessary facilities and academic support. The authors further acknowledge the SPPU Pune University for its support and academic framework.

DATA AVAILABILITY

Data acquisition and utilization procedures are described within the paper.

REFERENCES

[1] S. Ismail, D. W. Dawoud, and H. Reza, "Securing Wireless Sensor Networks Using Machine Learning and Blockchain: A Review," *Future Internet*, vol. 15, no. 6, May 2023, Art. no. 200, https://doi.org/10.3390/fi15060200.

[2] T. S. Delwar *et al.*, "The Intersection of Machine Learning and Wireless Sensor Network Security for Cyber-Attack Detection: A Detailed Analysis," *Sensors*, vol. 24, no. 19, Oct. 2024, Art. no. 6377, https://doi.org/10.3390/s24196377.

[3] V. Sivagaminathan, M. Sharma, and S. K. Henge, "Intrusion Detection Systems for Wireless Sensor Networks Using Computational Intelligence Techniques," *Cybersecurity*, vol. 6, no. 1, Oct. 2023, Art. no. 27, https://doi.org/10.1186/s42400-023-00161-0.

[4] Md. A. Talukder, M. Khalid, and N. Sultana, "A Hybrid Machine Learning Model for Intrusion Detection in Wireless Sensor Networks Leveraging Data Balancing and Dimensionality Reduction," *Scientific Reports*, vol. 15, no. 1, Feb. 2025, Art. no. 4617, https://doi.org/10.1038/s41598-025-87028-1.

[5] B. Mopuru and Y. Pachipala, "Advancing IoT Security: Integrative Machine Learning Models for Enhanced Intrusion Detection in Wireless Sensor Networks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14840–14847, Aug. 2024, https://doi.org/10.48084/etasr.7641.

[6] G. G. Gebremariam, J. Panda, and S. Indu, "Design of Advanced Intrusion Detection Systems Based on Hybrid Machine Learning Techniques in Hierarchically Wireless Sensor Networks," *Connection Science*, vol. 35, no. 1, Dec. 2023, Art. no. 2246703, https://doi.org/10.1080/09540091.2023.2246703.

[7] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, "Wireless Sensor Network Security: A Recent Review Based on State-of-the-Art Works," *International Journal of Engineering Business Management*, vol. 15, Feb. 2023, Art. no. 18479790231157220, https://doi.org/10.1177/18479790231157220.

[8] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," *Sensors*, vol. 22, no. 13, Jun. 2022, Art. no. 4730, https://doi.org/10.3390/s22134730.

[9] Y. Kumar and V. Kumar, "A Systematic Review on Intrusion Detection System in Wireless Networks: Variants, Attacks, and Applications," *Wireless Personal Communications*, vol. 133, no. 1, pp. 395–452, Nov. 2023, https://doi.org/10.1007/s11277-023-10773-x.

[10] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," *Journal of Information Security and Applications*, vol. 50, Feb. 2020, Art. no. 102419, https://doi.org/10.1016/j.jisa.2019.102419.

[11] Y. Meidan *et al.*, "ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis," in *Proceedings of the Symposium on Applied Computing*, Marrakech, Morocco, Apr. 2017, pp. 506–509, https://doi.org/10.1145/3019612.3019878.

[12] G. Kumar and H. Alqahtani, "Machine Learning Techniques for Intrusion Detection Systems in SDN-Recent Advances, Challenges and Future Directions," *Computer Modeling in Engineering & Sciences*, vol. 134, no. 1, pp. 89–119, 2023, https://doi.org/10.32604/cmes.2022.020724.

[13] B. R. Kikissagbe and M. Adda, "Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review," *Electronics*, vol. 13, no. 18, Sep. 2024, Art. no. 3601, https://doi.org/10.3390/electronics13183601.

[14] B. Al-Fuhaidi, Z. Farae, F. Al-Fahaidy, G. Nagi, A. Ghallab, and A. Alameri, "Anomaly-Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms," *Applied Computational Intelligence and Soft Computing*, vol. 2024, no. 1, Jan. 2024, Art. no. 2625922, https://doi.org/10.1155/2024/2625922.

[15] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software Defined Networks-Based Smart Grid Communication: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2637–2670, 2019, https://doi.org/10.1109/COMST.2019.2908266.

[16] K. Padmavathi and M. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1, pp. 1–9, 2009.

[17] S. K. Jagatheesaperumal, Q.-V. Pham, R. Ruby, Z. Yang, C. Xu, and Z. Zhang, "Explainable AI Over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 2106–2136, 2022, https://doi.org/10.1109/OJCOMS.2022.3215676.

[18] R. Mitchell and I.-R. Chen, "A Survey of Intrusion Detection Techniques for Cyber-physical Systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, Apr. 2014, https://doi.org/10.1145/2542049.

[19] Y. Xin *et al.*, "Machine Learning and Deep Learning Methods for Cybersecurity," *IEEE Access*, vol. 6, pp. 35365–35381, 2018, https://doi.org/10.1109/ACCESS.2018.2836950.

[20] D. Jeevaraj *et al*., "Intrusion Detection in WSN Using Supervised Machine Learning Techniques," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 9, pp. 483–490, 2023.

[21] Md. 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, Jun. 2024, https://doi.org/10.1007/s10207-024-00833-z.

[22] A. B. Abhale and A. J. Reddy, "Deep Learning Perspectives to Detecting Intrusions in Wireless Sensor Networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 2S, pp. 18–26, 2023.

[23] M. Supriya and T. Adilakshmi, "Intrusion Detection in Wireless Sensor Networks Using Histogram Gradient Boosting Classifier," in *Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 1*, vol. 1273, A. Kumar, V. K. Gunjan, S. Senatore, and Y.-C. Hu, Eds. Singapore: Springer Nature Singapore, 2025, pp. 473–480.

[24] S. M. S. Bukhari *et al.*, "Secure and Privacy-Preserving Intrusion Detection in Wireless Sensor Networks: Federated Learning With SCNN-Bi-LSTM for Enhanced Reliability," *Ad Hoc Networks*, vol. 155, Mar. 2024, Art. no. 103407, https://doi.org/10.1016/j.adhoc.2024.103407.

[25] S. Bhardwaj, S. Rawat, and H. B. Maringanti, "Intrusion Detection Utilizing an Ant Colony Optimization-Based Feature Selection and the XGBoost Classifier," *Engineering, Technology & Applied Science Research*, vol. 16, no. 2, pp. 32989–32994, Apr. 2026, https://doi.org/10.48084/etasr.14572.

[26] P. Selvam *et al.*, "Federated Learning-Based Hybrid Convolutional Recurrent Neural Network for Multi-class Intrusion Detection in IoT Networks," *Discover Internet of Things*, vol. 5, no. 1, Apr. 2025, Art. no. 39, https://doi.org/10.1007/s43926-025-00130-8.

[27] S. Agrawal *et al.*, "Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions." arXiv, 2021, https://doi.org/10.48550/ARXIV.2106.09527.

[28] K. P. Sharma *et al.*, "Interpretable Intrusion Detection for IoT Environments Using a Self-Attention-Based Explainable AI Framework," *Scientific Reports*, vol. 15, no. 1, Nov. 2025, Art. no. 39937, https://doi.org/10.1038/s41598-025-23750-0.

[29] H. Tabbaa, S. Ifzarne, and I. Hafidi, "An Online Ensemble Learning Model for Detecting Attacks in Wireless Sensor Networks," arXiv, 2022, https://doi.org/10.48550/ARXIV.2204.13814.

[30] K. Haseeb, N. Islam, T. Saba, A. Rehman, and Z. Mehmood, "LSDAR: A Light-Weight Structure Based Data Aggregation Routing Protocol with Secure Internet of Things Integrated Next-generation Sensor Networks," *Sustainable Cities and Society*, vol. 54, Mar. 2020, Art. no. 101995, https://doi.org/10.1016/j.scs.2019.101995.

[31] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics,"

IEEE Access, vol. 8, pp. 11743–11753, 2020, https://doi.org/10.1109/ACCESS.2019.2959047.

[32] K. Haseeb, K. M. Almustafa, Z. Jan, T. Saba, and U. Tariq, "Secure and Energy-Aware Heuristic Routing Protocol for Wireless Sensor Network," *IEEE Access*, vol. 8, pp. 163962–163974, 2020, https://doi.org/10.1109/ACCESS.2020.3022285.

[33] M. Hasan Ali and M. Atif Rasheed, "A Blockchain-Based Multi-Agent Security Framework for E-Commerce Systems," *International Journal of Theoretical & Applied Computational Intelligence*, pp. 228–245, 2025, https://doi.org/10.65278/IJTACI.2025.15.

[34] U. Suleiman Bichi and S. Bala Abdullahi, "Human Action Recognition: A Comprehensive Survey of Multimodal Advances, Challenges, and Emerging Directions," *International Journal of Theoretical and Applied Computational Intelligence*, pp. 305–322, 2025, https://doi.org/10.65278/IJTACI.2025.36.

AUTHORS PROFILE

Sumedh Dhengre is an Assistant Professor in Computer Engineering at AISSMS College of Engineering, Pune, with over 17 years of teaching experience. He is currently pursuing a Ph.D. at Savitribai Phule Pune University. His research interests include Wireless Sensor Networks, Machine Learning, and Intrusion Detection Systems. He has published several papers in international journals and conferences, and holds international and national patents in his research domain.

Shabnam Sayyad is an academician and researcher in the field of Computer Engineering, with expertise in Machine Learning, Network Security, and Wireless Sensor Networks. She holds a doctoral degree and has contributed to several research publications in reputed journals and conferences. Her research focuses on intelligent security mechanisms, data-driven models, and advanced computing techniques. She is actively involved in teaching, research guidance, and academic development activities, with a strong interest in emerging technologies and their real-world applications.