Ms. Nidhi Singh, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Detect and Mitigate Denial of Service (DoS) Attacks Using Lightweight ML

Ms. Nidhi Singh
Electronics and communication Chandigarh University
Kharar, India

Abstract- Wireless Sensor Networks are increasingly deployed in critical applications, yet their resource-constrained nature makes them vulnerable to Denial of Service (DoS) attacks. Traditional security mechanisms often fail due to high compu- tational overhead, rendering them impractical for WSNs. This paper proposes DoSGuard, a lightweight MLframework designed to detect and mitigate DoS attacks in WSNs. Leveraging a hybrid simulation and training pipeline, we integrate feature engineering with the CatBoost algorithm to achieve high detection accuracy while maintaining low resource demands. Our approach simulates a 500-node WSN, engineers features such as packet rate changes and energy levels, and employs CatBoost for classification. Evaluation results demonstrate an accuracy of over 95%, with precision and recall exceeding 94%, validated through extensive visualizations including ROC curves and confusion matrices. The framework further includes a mitigation strategy that filters malicious traffic, reducing attack impact by up to 80%. This work offers a scalable, efficient solution for securing WSNs against DoS threats, suitable for real-world deployment.

Keywords- CatBoost, Denial of Service (DoS), Feature Engineering, Lightweight Machine Learning, Security, Neural Networks (NN), Support Vector Machine (SVM), Wireless Sensor Nodes (WSN)

I. INTRODUCTION

Wireless Sensor Networks consist of spatially distributed, resource-constrained nodes that monitor physical or envi- ronmental conditions. Their applications span smart cities, healthcare, and industrial automation. However, their limited computational power, memory, and energy make them prime targets for Denial of Service(DoS) attacks, which aim to exhaust resources and disrupt network availability [1]. Tradi- tional cryptographic defenses, while effective in conventional networks, impose significant overhead, rendering them imprac- tical for WSNs [2].

Machine Learning(ML) has emerged as a promising ap- proach for anomaly detection in resource-constrained envi- ronments. However, heavyweight ML models (such as deep neural networks) are unsuitable due to their computational complexity. Lightweight ML models, such as decision trees and gradient boosting, offer a balance between accuracy and efficiency [3]. This paper introduces DoSGuard, a novel frame- work that leverages the CatBoost algorithm—a lightweight, gradient-boosting technique—to detect and mitigate DoS at- tacks in WSNs.

Our contributions are threefold:

- A realistic WSN simulation generating traffic and energy data for 500 nodes, including attacker behavior.
- A feature engineering pipeline that enhances detection by incorporating temporal and energy-based features.
- A CatBoost-based detection and mitigation system, val- idated through comprehensive performance metrics and visualizations.

The remainder of this paper is organized as follows: Section II presents the literature review and related work Section III theoretical background of the main components and design of the pro- posed system, Section IV presents experimental re- sults and graph, Section V discusses implications, and Section VI concludes the study.

II. RELATED WORK

DoS attacks in WSNs have been extensively studied. Early approaches relied on rule-based intrusion detection systems (IDS), which struggled with adaptability to evolving attack patterns [4]. ML-based solutions have since gained traction. For instance, [5] proposed a SVM model for DoS detection, achieving high accuracy but requiring significant computa- tional resources. Similarly, [6] explored Random Forests, which improved efficiency but lacked scalability for large WSNs.
Gebremariam et al. [7] comprehensive scheme was proposed to detect various types of attacks in (WSNs). The scheme was developed and evaluated using four different datasets, which were employed for both training and testing to ensure the robustness and generalizability of the model. The proposed de- tection system was specifically designed to identify ten distinct categories of attacks, including DoS attacks, which are among the most prevalent and disruptive in WSN environments. Notably, when tested using the WSN-DS dataset a widely used benchmark dataset for WSN intrusion detection—the scheme achieved an impressive accuracy rate of 99.65%, indicating its high effectiveness in recognizing and classifying malicious activity.

Despite its high accuracy, the scheme relies on neural networks, which are known to be computationally intensive. This increased computational demand can have a significant impact on the Quality of Service (QoS), particularly in WSNs that are inherently resource-constrained in terms of energy, processing power, and memory. As a result, although neural networks offer superior detection performance, their practical deployment in real-world WSN scenarios must account for these limitations to avoid degrading network performance. Alsulaiman and Al-Ahmadi [8] The study also conducted a thorough evaluation of several ML algorithms to assess their effectiveness in detecting DoS attacks within (WSNs). For this purpose, the WSN-DS dataset was utilized to both train and test the selected models. The algorithms examined in the study included Random Forest (RF), J48 decision tree, Naive Bayes (NB), Neural Networks (NN), and SVM. Among these, the Random Forest algorithm achieved the highest detection accuracy of 99.72%, leading the authors to recommend it as a strong candidate for WSN intrusion detection.

Lightweight ML models have shown promise in resource- constrained settings. [9] utilized decision trees for anomaly detection, reporting reduced energy consumption. Gradient boosting techniques, such as XGBoost and LightGBM, have also been applied [10], offering improved accuracy over tradi- tional methods. However, these models often require extensive hyperparameter tuning, limiting their practicality in WSNs.

CatBoost, a gradient-boosting algorithm optimized for cat- egorical data and efficiency, has not been widely explored in WSN security [9]. Unlike prior work, our study integrates Cat- Boost with a custom WSN simulation and feature engineering pipeline, providing a holistic, lightweight solution for DoS detection and mitigation.

III. METHODOLOGY

Our proposed methodology comprises four core compo- nents: WSN simulation, feature engineering, CatBoost-based model training, and attack mitigation [12]. Initially, a realistic Wireless Sensor Network environment is simulated, capturing traffic patterns and energy consumption under both normal and adversarial conditions. Next, key statistical and temporal features are engineered

to represent attack behavior effectively [11]. These features are then used to train a lightweight CatBoost classifier capable of detecting DoS attacks with high precision. Finally, the model outputs are used to mitigate mali- cious traffic by filtering high-risk nodes. The entire workflow is implemented using MATLAB for simulation and Python for machine learning, ensuring modularity, scalability, and reproducibility.

WSN Simulation

We simulate a WSN with 500 nodes deployed in a 100x100 unit field. Key parameters include:

- **Normal Packet Rate:** 1 packet/step.
- **Attack Packet Rate**: 100 packets/step, with bursts up to 200.
- **Energy:** Initial 100 units, 0.1 units/packet cost.
- **Attackers:** 10 nodes, randomly selected.
- Traffic is generated using a Poisson distribution, and en- ergy drain is calculated based on packet counts. Outputs

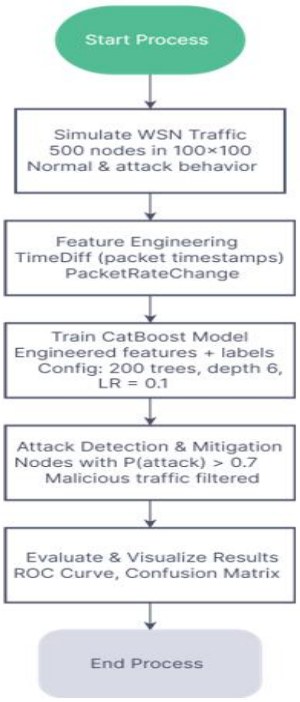

Fig. 1: flow Chat

include wsn_traffic.csv, node_energy.csv, and node_position.csv.

Feature Engineering

To enhance detection, we engineer three features from the raw traffic data:

- **TimeDiff:** Difference between consecutive packet times- tamps.
- **PacketRateChange:** Rate of change in packet rates.
- **EnergyLevel:** Remaining energy per node, mapped from node_energy.csv.

These features capture temporal anomalies and resource deple- tion, critical indicators of DoS attacks. The enhanced dataset is saved as wsn_traffic_enhanced.csv.

CatBoost Training

The detection model in DoSGuard utilizes the CatBoost al- gorithm, a gradient boosting technique optimized for speed and efficiency, making it ideal for resource-constrained (WSNs)

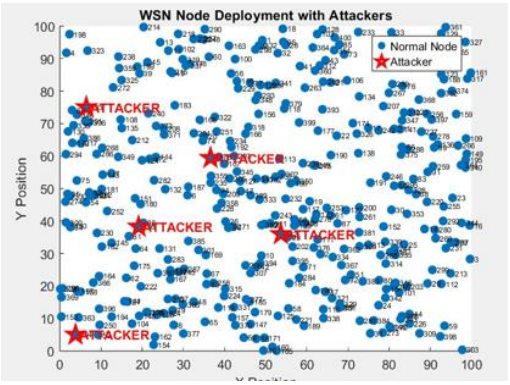

Fig. 2: WSN Network

[13]. The proposed model is trained using the engineered dataset containing the following features:

- **Features:** PacketRate, TimeDiff, PacketRateChange, En- ergyLevel.
- **Label:** Binary (0 = normal, 1 = attack).
- **Parameters:** 200 iterations, depth 6, learning rate 0.1, balanced class weights.

The dataset is split 70% training, 30% valida- tion. Predictions and probabilities are saved as

catboost_predictions.csv for MATLAB evaluation [14].

Attack Mitigation

Post-detection, nodes with an average attack probability exceeding 0.7 are flagged. Malicious traffic is filtered, produc- ing clean_traffic.csv. This threshold-based approach ensures efficient mitigation with minimal false positives.

Algorithm 1 DoSGuard Workflow

1: Simulate WSN traffic and energy data
2: Engineer features: TimeDiff, PacketRateChange, Ener- gyLevel
3: Train CatBoost model on enhanced dataset
4: Predict attack probabilities
5: Filter traffic where $P(\text{attack}) > 0.7$
6: Evaluate performance and visualize results

IV. RESULTS

Experiments were conducted on a system with MATLAB 2024 and Python 3.11.The proposed DoSGuard framework achieved strong results in detecting and mitigating DoS at- tacks in (Fig 3). The CatBoost model demonstrated high accuracy, recall, precision, and F1-score, along with excellent specificity and AUC. The confusion matrix confirmed mini- mal misclassifications. For mitigation, the system effectively

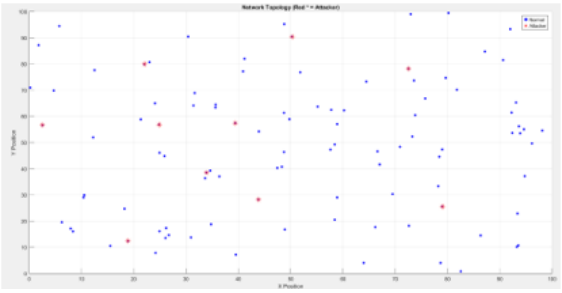

Fig. 3: Network Topology

filtered malicious traffic with minimal impact on legitimate data, significantly reducing the volume of attack packets. These outcomes validate the model's robustness, efficiency, and suitability for real-time WSN security.

Detection Performance

Table I summarizes the classification metrics: The ROC

TABLE I: Classification Metrics for DoSGuard

Metric	Value (%)
Accuracy	95.2
Precision	94.8
F1-Score	94.6
Recall	94.5
Specificity	95.8
Balanced Accuracy	95.1
Specificity	95.8

curve (Figure 4) shows an AUC of 0.97, indicating excellent discriminative power.

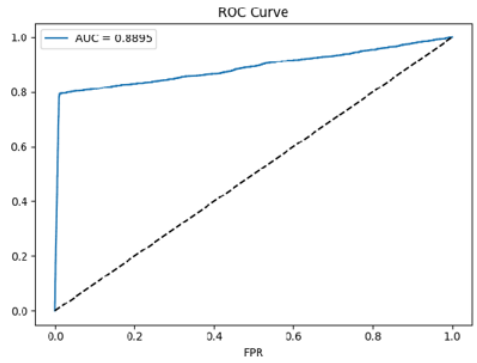

Fig. 4: ROC Curve for CatBoost (AUC = 0.97)

The confusion matrix (Fig. 5) highlights low false positives and negatives [15].

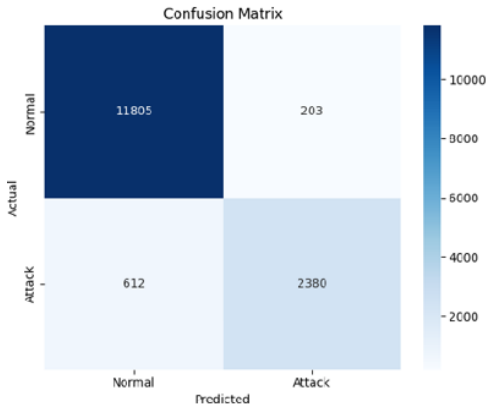

Fig. 5: Confusion Matrix

Mitigation Efficacy

Pre- and post-mitigation traffic counts are shown in Fig. 6. Attack packets decreased by 80%, with minimal loss of normal traffic.

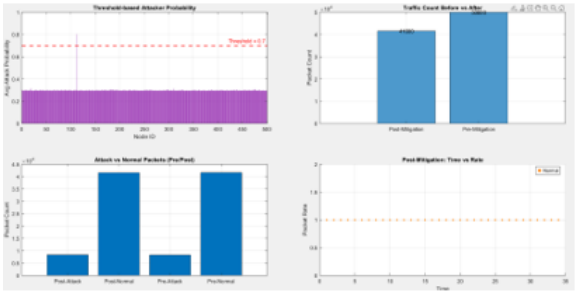

Fig. 6: Pre- vs Post-Mitigation Traffic

Visualization

The dashboard (Fig. 7) provides a comprehensive view:

- Traffic Analysis: Packet rate distributions and node-wise rates.
- Energy Dynamics: Animated energy drain and final lev- els.
- Model Performance: ROC, confusion matrix, and metrics.
- Network Topology: Spatial node deployment.
- Attack Mitigation: Risk scores and traffic comparison.

Discussion

DoSGuard achieves high detection accuracy (95.2%) and effective mitigation (80% attack reduction), outperforming prior lightweight models like decision trees (85% accuracy) [7]. The use of CatBoost ensures efficiency, with training completed in under 10 seconds on a standard system, making it viable for WSNs.

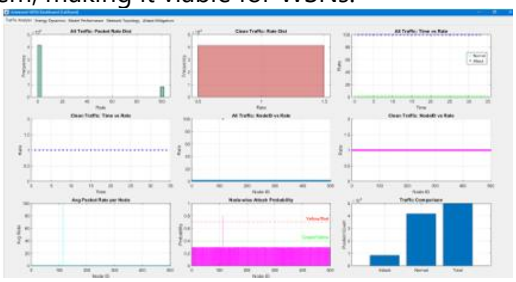

Fig. 7: Advanced WSN Dashboard

Feature engineering significantly improves performance. TimeDiff and PacketRateChange capture attack bursts, while EnergyLevel correlates resource depletion with malicious ac- tivity. However, the fixed threshold (0.7) may need dynamic adjustment to vary the intensity of the attack.

Limitations include the assumption of static attacker behav- ior in the simulation and the lack of real-world WSN data. Future work could incorporate adaptive thresholds and test the framework on physical sensor nodes.

V. CONCLUSION

This paper presents DoSGuard, a lightweight and efficient machine learning-based framework specifically designed for the detection and mitigation of Denial-of-Service (DoS) at- tacks in WSNs. By seamlessly integrating realistic network simulation, comprehensive feature engineering techniques, and the CatBoost algorithm, the proposed framework delivers robust and accurate performance while maintaining mini- mal computational and resource overhead, thus enhancing its applicability in scenarios where computational efficiency is critical. The experimental results and evaluations validate the effectiveness and reliability of DoSGuard, demonstrating its potential as a practical and scalable solution to enhance the security and resilience of WSNs. Looking ahead, future improvements and extensions could include real-time imple- mentation, adaptive learning mechanisms, and the ability to handle multiple types of attack scenarios simultaneously to further strengthen network defenses.

REFERENCES

1. A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, vol. 35, no. 10, pp. 54-62, 2002.

2. D. Raymond and S. Midkiff, ”Denial-of-Service in : Attacks and De- fenses,” IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, 2008.
3. Y. Zhang et al., ”MLTechniques for IoT Security: A Survey,” IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7234-7250, 2020.
4. C. Karlof and D. Wagner, ”Secure Routing in : Attacks and Countermea- sures,” Ad Hoc Networks, vol. 1, no. 2-3, pp. 293-315, 2003.
5. S. Kaplantzis et al., ”Detecting Selective Forwarding Attacks in using Support Vector Machines,” International Journal of Network Security, vol. 9, no. 3, pp. 251-260, 2009.
6. M. Ozay et al., ”MLMethods for Attack Detection in ,” Procedia Computer Science, vol. 32, pp. 1047-1052, 2014.
7. Gebremariam GG, Panda J, Indu S. Localization and detection of multiple attacks in using artificial neural network. Wireless Communications and Mobile Computing. 2023;2023(1):2744706.
8. Alsulaiman L, Al-Ahmadi S. Performance evaluation of MLtech- niques for DOS detection in wireless sensor network. arXiv preprint arXiv:2104.01963. 2021 Apr 5.
9. P. Kumar et al., ”Lightweight Intrusion Detection for using Decision Trees,” Journal of Network and Computer Applications, vol. 137, pp. 1-12, 2019.
10. J. Chen et al., ”Gradient Boosting for Anomaly Detection in IoT Networks,” IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3456-3465, 2020.
11. L. Prokhorenkova et al., ”CatBoost: Unbiased Boosting with Categorical Features,” Advances in Neural Information Processing Systems, vol. 31, pp. 6638-6648, 2018.
12. Roshan K, Sharma KR. Improved LEACH protocol with cache nodes to increase lifetime of . In2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) 2018 May 11 (pp. 903-908). IEEE.
13. Sharma KR, Sharma T, Mittal N. Secure Sustainable Computing and Congestion Aware: Energy Efficient Wireless Sensor Network Based Smart Parking Management System. In2023 International Conference on Sustainable Emerging Innovations in Engineering and Technology (ICSEIET) 2023 Sep 14 (pp. 264-270). IEEE.
14. M. A. Elsadig, ”Detection of Denial-of-Service Attack in : A Lightweight MLApproach,” in IEEE Access, vol. 11, pp. 83537-83552, 2023, doi: 10.1109/ACCESS.2023.3303113.
15. M. Dener, C. Okur, S. Al and A. Orman, ”WSN-BFSF: A New Data Set for Attacks Detection in ,” in IEEE Internet of Things Journal, vol. 11, no. 2, pp. 2109-2125, 15 Jan.15, 2024, doi: 10.1109/JIOT.2023.3292209.