RESEARCH PAPER

Deep Learning based Intrusion Detection for Mitigating Denial of Service Attacks in Wireless Sensor Networks

R. Usha Devi[1], Dr. R. Kannan[2]

[1] Ph.D Research Scholar, Department of Computer Science, SRMV College of Arts & Science, Coimbatore - 49. Email: usha121196@gmail.com

[2] Associate Professor, Department of Computer Science, SRMV College of Arts & Science, Coimbatore - 49

ABSTRACT

Wireless Sensor Networks (WSNs) are increasingly targeted by Denial-of-Service (DoS) attacks, which compromise network integrity through resource exhaustion and protocol manipulation. To address the limitations of conventional intrusion detection systems (IDS) in dynamic WSN environments, this paper proposes a novel deep learning (DL) framework synergized with metaheuristic optimization. We integrate five DL architectures such as Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), Gated Recurrent Units (GRUs), Long Short-Term Memory (LSTM), and Transformers with advanced optimization techniques, including Grid Search (GS), Bat Algorithm (BA), Cuckoo Search (CS), Sparrow Search Algorithm (SSA), and a newly developed Quantum Search-Enhanced Bat Algorithm (QS-BAT). Evaluated extensively on the WSN-DS dataset, which emulates real-world attack scenarios (Blackhole, Grayhole, Flooding, Scheduling), our approach demonstrates superior detection robustness, adaptability, and computational efficiency. The framework significantly outperforms existing methods, establishing a new benchmark for high-precision, real-time intrusion detection in resource-constrained WSNs.

Keywords: Wireless Sensor Networks, Intrusion Detection System, Deep Learning, Metaheuristic Optimization, QS-BAT.

How to cite this article: Usha Devi R, Kannan R. Deep Learning based Intrusion Detection for Mitigating Denial of Service Attacks in Wireless Sensor Networks. Int J Drug Deliv Technol. 2026;16(23s): 720-734. DOI: 10.25258/ijddt.16.23s.78

Source of support: Nil.

Conflict of interest: None

1. Introduction

Wireless Sensor Networks (WSNs) play a vital role in a wide range of applications, including healthcare monitoring, industrial automation, and environmental surveillance. Their decentralized architecture and limited computational resources make them particularly vulnerable to Denial-of-Service (DoS) attacks such as Blackhole, Grayhole, Flooding, and Scheduling attacks. These attacks can severely impact routing efficiency, drain energy resources, and compromise the reliability and security of transmitted data [1].

Traditional IDS based on static signatures struggle to adapt to the evolving nature of these threats. Similarly, conventional machine learning methods often require large volumes of labeled data, which is not always feasible in dynamic and resource-constrained WSN environments. DL offers a promising alternative due to its ability to learn complex patterns and detect anomalies with high accuracy. However, designing effective DL-based IDS for WSNs remains challenging due to the need for optimal hyperparameter tuning and the computational limitations of sensor nodes. This necessitates the integration of efficient optimization techniques. This paper introduces a hybrid deep learning and optimization framework for detecting DoS attacks in WSNs. The key contributions include:

- Development and comparison of five deep learning architectures (CNN, GAN, GRU, LSTM, Transformer) designed to capture spatial, temporal, and adversarial behaviors in WSN traffic.
- Implementation of advanced hyperparameter optimization methods, including Grid Search, Bat Algorithm, Cuckoo Search, Sparrow Search Algorithm, and a novel Quantum Search-Enhanced Bat Algorithm (QS-BAT).

- A comprehensive evaluation using a large-scale WSN dataset with real-world attack scenarios based on the LEACH routing protocol.

- Achievement of state-of-the-art detection performance with high accuracy and minimal false positives, demonstrating the effectiveness of the proposed framework.

The remainder of the paper is organized as follows: Section 2 presents the related work. Section 3 outlines the proposed methodology, including model design and optimization techniques. Section 4 describes the experimental setup and dataset. Section 5 discusses the results and performance analysis. Finally, Section 6 concludes the paper with insights and future directions.

2. Literature review

Hussain et al. (2024) proposed a Deep Q-Network (DQN) based cyber-attack detection system that overcomes the limitations of supervised learning by learning directly from network traffic without relying on labeled data or fixed signatures. Their model includes an adversarial training mechanism where a secondary DQN agent generates perturbed data to improve detection robustness. Evaluated on benchmark datasets, the DQN model achieved an accuracy of 98.7% and a false positive rate of 1.8%, outperforming convolutional neural network (CNN) and multilayer perceptron (MLP) models in both accuracy and false positives. This approach demonstrates strong potential for adaptive and effective intrusion detection in dynamic network environments [2].

Kim et al. (2025) investigate the application of Machine Learning (ML) and Deep Learning (DL) techniques to enhance cybersecurity in script development, addressing the growing complexity of threats in modern software environments. Utilizing the Fashion MNIST dataset, the study implements a CNN model to demonstrate the potential of ML/DL methodologies in automating security analysis and threat mitigation within the software development lifecycle. Key phases such as data preprocessing, model training and evaluation through accuracy and loss metrics are meticulously executed. The results reveal a substantial improvement in cybersecurity performance, with the CNN model achieving an accuracy of 92.4% and a loss value reduced to 0.15, thereby validating the effectiveness of this approach in strengthening software resilience. This research contributes to cybersecurity literature by highlighting practical integration strategies of ML and DL in real-world script development, offering developers a robust framework to counteract evolving security threats effectively [3].

Gueriani, et.al (2025) address the escalating cybersecurity challenges in the Industrial Internet of Things (IIoT) by developing an advanced intrusion detection system (IDS) utilizing a hybrid LSTM-CNN Attention DL architecture. Their model targets both binary and multi-class classification tasks to accurately detect and categorize cyber-attacks within IIoT environments. Leveraging the Edge IIoTset dataset, the study effectively handles class imbalance through the application of Synthetic Minority Over sampling Technique (SMOTE), enhancing model training across underrepresented classes. Comparative experiments with various DL models demonstrate that the proposed LSTM-CNN-Attention architecture outperforms alternatives, achieving near perfect accuracy of 99.89% in binary classification and 99.04% accuracy with a loss value of 0.0220 in multi-class classification. These results underscore the model's robustness and precision in identifying diverse cyber threats, highlighting its suitability for securing critical IIoT infrastructures against increasingly sophisticated attacks [4].

Nandhini, et.al (2024) present a comprehensive research on cyber-attack detection in IoT-enabled Wireless Sensor Networks (IoT-WSN) by proposing optimized neural network algorithms, including Equilibrium Optimizer Neural Network (EO-NN), Particle Swarm Optimization Neural Network (PSO-NN), Single Candidate Optimizer Neural Network (SCO-NN), and Single Candidate Optimizer Long Short Term Memory (SCO-LSTM). Addressing a key limitation of existing IDS that fail to detect attacker nodes with dynamic behavior changes, their models focus on identifying nodes that shift from normal to malicious behavior due to continuous internet connectivity. The study utilizes threat intelligence data and explores various neural network architectures with different hidden and connected layers to enhance detection accuracy. Experimental results demonstrate that the SCO-LSTM model achieves superior classification accuracy rates of 99.7% without threat intelligence and 99.89% with threat intelligence,

along with a false positive rate reduction to 0.8%, indicating the effectiveness of the proposed approach in adapting to evolving attack patterns within IoT-WSN environments. This work significantly advances IDS capabilities by enabling dynamic behavior detection in complex networked sensor systems [5].

Behiryet.al (2024) proposes an intelligent hybrid model integrating ML and artificial intelligence to improve cyber-attack detection in WSNs. The study employs advanced feature reduction techniques, including Singular Value Decomposition (SVD) and Principal Component Analysis (PCA), combined with a K-means clustering model enhanced by information gain (KMC-IG) for efficient feature extraction. To address class imbalance, the Synthetic Minority Excessively Technique is applied, enhancing the quality of training data for intrusion detection and network traffic classification. The research rigorously evaluates a DL based feed forward neural network across three benchmark datasets NSL-KDD, UNSW-NB15, and CICIDS 2017 using both full and reduced feature sets. Results indicate that the proposed model achieves high accuracy rates of 98.3% on NSL-KDD, 97.6% on UNSW-NB15, and 98.9% on CICIDS 2017, alongside strong precision, recall, and F-measure scores, outperforming conventional ML approaches. This work substantially contributes to enhancing WSN security by providing an optimized, reliable intrusion detection framework capable of handling large scale, imbalanced datasets effectively [6].

Reza (2024) addresses the critical challenge of Distributed Denial of Service (DDoS) attacks in WSNs by proposing DDoS-Net, a hybrid DL model combining Long Short Term Memory (LSTM) and Multi-Layer Perceptron (MLP) architectures. The model is specifically designed to tackle the inherent data imbalance in WSN datasets and incorporates comprehensive feature analysis to enhance detection accuracy. Evaluated on the WSN-BFSF dataset, DDoS-Net demonstrates superior performance with an accuracy of 98.12%, precision of 98.16%, recall of 98.12%, and an f1-score of 0.98, achieved within minimal training epochs. These results outperform existing state-of-the-art intrusion detection methods, underscoring the model's robustness and effectiveness in mitigating DDoS threats in WSN environments. This study significantly contributes to advancing security frameworks for WSNs by offering an adaptive and high performing DL based detection system [7].

Sathishkumar, et.al (2024) presents an innovative intrusion detection framework for WSNs targeting Denial-of-Service (DoS) attacks by integrating fuzzy logic with a LSTM network. Their approach leverages temporal constraints and fuzzy rulebased weight fitting to enhance decision-making accuracy, alongside a Crow Search Algorithm (CSA) for dynamic feature selection that optimizes feature efficiency and reduces processing overhead. The model facilitates collaborative training across multiple sensor nodes while preserving data privacy, effectively addressing sophisticated and emerging cyber threats through analysis of local and temporal network correlations. Evaluated on the KDDCup99 and NSL-KDD datasets, the proposed FL-LSTM model achieves superior performance metrics with an accuracy of 99.58%, precision of 98.42%, recall of 98.45%, and an f1-score of 98.36%, outperforming conventional algorithms. This research significantly advances WSN security by providing a robust, privacy-aware, and high-precision detection mechanism tailored for complex DoS attack scenarios [8].

Fares, et. al(2025) investigate the application of Deep Neural Networks (DNN) for enhancing security in Wireless Sensor Networks (WSNs) by focusing on the detection of Denial-of-Service (DoS) attacks. Utilizing the WSN-DS dataset which includes diverse DoS attack types such as Blackhole, Grayhole, Flooding, and TDMA the study evaluates the DNN model's efficacy using standard performance metrics including accuracy, precision, recall, and F1-score. The experimental results demonstrate the model's strong capability in identifying DoS attacks, achieving a high accuracy rate of 97.85%, along with robust precision and recall values exceeding 97%, underscoring the effectiveness of deep learning techniques in safeguarding WSN environments against critical security threats. This research highlights the potential of DNNs as reliable components in modern intrusion detection systems tailored for the complex and dynamic nature of wireless sensor networks [9].

VanlalruataHnamte et al. (2024) propose a robust Deep Neural Network (DNN) framework for detecting and mitigating Distributed Denial-of-Service (DDoS) attacks within Software-Defined Network (SDN) environments, addressing the escalating complexity and sophistication of contemporary cyber threats. The model is designed to

analyze network traffic meticulously, identifying subtle attack patterns through scalable and adaptable deep learning techniques. Evaluation across multiple real world datasets InSDN, CICIDS2018, and KaggleDDoSdemonstrates exceptional detection accuracy of 99.98%, 100%, and 99.99%, respectively, along with consistently low loss rates, thereby outperforming traditional DDoS detection approaches. This research highlights not only the efficacy of DNNs in enhancing SDN security architectures but also discusses practical deployment challenges, providing critical insights for network security practitioners aiming to strengthen digital infrastructures against evolving DDoS threats [10].

Kandasamy and Roseline (2025) address the critical challenge of detecting Man-in-the-Middle (MitM) attacks within smart home environments, where the proliferation of connected devices has heightened security vulnerabilities. Their research introduces the AEXB Model, a novel hybrid DL approach that synergizes the unsupervised feature extraction capabilities of an AutoEncoder with the supervised classification strength of XGBoost. This combined methodology effectively enhances detection accuracy while reducing false positives, crucial for real-time intrusion detection. The research employs comprehensive preprocessing and feature selection techniques including Recursive Feature Elimination and correlation analysis applied to the Intrusion Detection in Smart Home (IDSH) dataset. The model achieved a notable accuracy of 97.24%, demonstrating its robust performance in identifying anomalous network behaviors associated with MitM attacks. Furthermore, the AEXB Model's ability to operate in real-time highlights its practical applicability for continuous threat monitoring in dynamic IoT ecosystems, making a significant contribution to advancing adaptive cybersecurity defenses in smart homes [11].

3. Materials and Methodology

This research employs a dual-phase methodology integrating advanced hyperparameter optimization with diverse deep learning architectures for DoS attack detection in WSNs. Five metaheuristic algorithms such as Grid Search (GS), Bat Algorithm (BA), Cuckoo Search (CS), Sparrow Search Algorithm (SSA), and a novel Quantum Search-Enhanced Bat Algorithm (QS-BAT) are leveraged to optimize hyperparameters (e.g., learning rate, layers, batch size) of five deep learning models: Convolutional Neural Networks (CNNs) for spatial pattern recognition, Generative Adversarial Networks (GANs) for adversarial training and data augmentation, Gated Recurrent Units (GRUs) and Long Short-Term Memory (LSTM) networks for temporal dependency modeling, and Transformers for long-range sequence analysis. The optimization process systematically navigates the parameter space to maximize detection metrics (accuracy, F1-score), with QS-BAT introducing quantum-inspired mechanisms for accelerated convergence. This hybrid approach enables robust feature extraction from the WSN-DS dataset while maintaining computational efficiency critical for resource-constrained sensor networks.

3.1HyperparameterOptimization

In intrusion detection for WSN hyperparameteroptimization improves the performance of DL models against DoSassaults. Grid Search does comprehensive tuning; nonetheless, it is computationally intensive. Metaheuristic algorithms such as the Bat Algorithm (BA), Cuckoo Search (CS), and Sparrow Search Algorithm (SSA)provide effective parameter optimization. A suggested Quantum Search Enhanced Bat Algorithm(QS-BAT) enhances convergence and precision. It adeptly equilibrates exploration and exploitation. These refined parameters enhance detection precision and diminish false positives.

i. Grid search (GS): GSis a hyper parameter optimization technique used to identify the best parameter configuration for DL models designed to DoS attacks in WSNs. It systematically explores combinations of hyper parameterssuch as learning rate, number of layers, neurons per layer, and batch size to maximize model performance. Despite being computationally intensive, grid search is easily parallelizable due to the independence of parameter combinations. Applied to DoS detection datasets, grid search identifies optimal hyper parameters to enhance accuracy and detection efficiency. The process can be mathematically defined as:

$$\theta^* = arg \max_{\theta \epsilon \Theta} \mathcal{M}(f(x;\theta))$$

Where, θ denotes a specific set of hyper parameters from the space, $f(x;\theta)$ is the model trained with θ, $\mathcal{M}(\cdot)$is the evaluation metric (e.g., accuracy or F1-score), and θ^* represents the optimal hyper

parameter set. This ensures the DL model is fine-tuned for precise and reliable detection of DoS attacks in WSNs [12].

ii. Bat Algorithm (BA): The BAoptimizes hyper parameters of DL models designed to detect and mitigate DoS attacks in WSNs. Each bat represents a candidate hyper parameter set within a d-dimensional search space. The updates are given by:

$$f_i = f_{min} + (f_{max} - f_{min})\,\beta, \qquad \beta \in [0,1]$$

$$\mathcal{V}_i^t = \mathcal{V}_i^{t-1} + (x_i^{t-1} - x^*) f_i$$

$$x_i^t = x_i^{t-1} + \mathcal{V}_i^t$$

Where, f_i: Frequency of bat i,x_i^t: position of bat i at iteration t,$\mathcal{V}_i^t$: velocity of bat i at iteration t,x^* : global best solution found so far, β: random vector drawn from a uniform distribution $[0,1]$, f_{min}, f_{max}: minimum and maximum frequency bounds, so far. Loudness and pulse emission rates are updated as:

$$A_i^{t+1} = \alpha A_i^t, r_i^{t+1} = r_i^0[1 - \exp(-\gamma t)]$$

Where, $\alpha \in (0,1)$: damping factor for loudness, $\gamma > 0$: constant controlling the increase in pulse emission rate,r_i^0: initial pulse rate [13].

iii. Cuckoo Search (CS): The CS is a nature inspired metaheuristic optimization algorithm modeled on the parasitic reproduction strategy of cuckoo birds. In DL based intrusion detection systems for mitigating DoS attacks in WSNs, CS is employed to optimize hyper parameters, thereby enhancing detection accuracy and efficiency. Each candidate solution represents a potential set of hyper parameters, such as learning rate, number of layers, and batch size. New solutions are generated through Lévy flights, which promote a balance between exploration and exploitation and help escape local optima. The generation of a new solution is governed by the equation:

$$x_i^{(t+1)} = x_i^{(t)} + \alpha \cdot Lévy(\lambda)$$

Where x_i^t is the current solution, $\alpha$is the step size, and $Lévy(\lambda)$ denotes a Lévy flight distribution with $1 < \lambda \leq 3$. Additionally, poor solutions are abandoned with a certain probabilityp_a, and replaced using:

$$x_i^{(t+1)} = RandomInitialization\ ()\ if\ rand\ < p_a$$

This mechanism enables the algorithm to continuously refine the DL model by discarding less effective parameter combinations. Through this approach, the IDS benefits from higher detection rates and reduced false positive occurrences, making CS a valuable tool for optimizing security solutions in dynamic and resource-constrained WSN environments [14].

iv. Sparrow Search Algorithm (SSA): The SSA is a swarm based optimization method inspired by the foraging and anti-predator behavior of sparrows. In DL based IDS for mitigating DoS attacks in WSNs, SSA optimizes hyper parameters of deep neural networks. Each sparrow represents a candidate solution in the search space. The position of discoverer sparrows is updated by:

$$X_{i,j}^t = \begin{cases} X_{i,j}^t \,.\, e^{-i \cdot \frac{\alpha}{iter_{max}}}, & W < ST \\ X_{i,j}^t + Z \,.\, L, & W \geq ST \end{cases}$$

Where,$W \in [0,1]$,$ST \in [0.5,1]$ and Z, L are random factors representing environmental influences. Follower sparrows update their position as:

$$X_{i,j}^{t+1} = \begin{cases} z \,.\exp\left(\frac{X_{worst}^t - X_{i,j}^t}{i^2}\right), & i > n/2 \\ X_p^{t+1} + \left|X_{i,j}^t - X_p^{t+1}\right| \,.\, A^+ + L, & otherwise \end{cases}$$

and also

$$X_{i,j}^{t+1} = \begin{cases} X_{best}^t + \beta \,.\, \left|X_{i,j}^t - X_{best}^t\right|, i > n/2 \\ X_{i,j}^t + \dfrac{\left|X_{i,j}^t - X_{worst}^t\right|}{f_i - f_w + \epsilon}, & otherwise \end{cases}$$

These equations enable SSA to effectively explore and exploit the search space, enhancing the performance of DL models for detecting and mitigating DoS attacks in WSNs [15].

v. Quantum Search Enhanced Bat Algorithm (QS-BAT): The Quantum Search-Enhanced Bat Algorithm (QS-BAT) is a hybrid metaheuristic designed to solve global optimization problems by integrating quantum inspired search with the standard bat algorithm. The objective function is defined as $f(x_i)$, where $x_i = (x_{i1}, \ldots\ldots, x_{iD})^\top$), represents a solution in a Ddimensional space. The algorithm initializes a population $x_i$and corresponding velocitiesv_i, with each bat assigned a frequency $Q_i \in [Q_{min}, Q_{max}]$, pulse rate$r_i \in [r_{min}, r_{max}]$and loudness$A_i \in [A_{min}, A_{max}]$. An elite archive of size k

is used to retain top performing solutions. A quantum comparator $cmp(x) = \mathbb{I}[f(x) < f(x^*)]$ identifies better solutions than the current global bestx^*. Each bat updates its frequency using $Q_i \in [Q_{min}, Q_{max}] \cdot rand(0,1)$, velocity via$v_i^{t+1} = v_i^t + (x_i^t - x^*) \cdot Q_i$and position with $x_i^{t+1} = x_i^t + v_i^{t+1}$. If $rand(0,1) > r_i$ a quantum exponential search is performed around x^*, and the new solution $x_{new}$is evaluated. If $rand(0,1) < A_i$ and $f(x_i) < f(x*)$, the new position is accepted. Parameters are adapted using$r_i = r_{i0}(1 - e^{-\gamma t})$ and $A_i = A_i \alpha^t$. The global best $x^*$is updated, and mutation is applied to the top 10% of solutions to maintain diversity. The process continues until the maximum iteration $T_{max}$is reached, and the best solution $x^*$is returned.

Algorithm: Quantum Search Enhanced Bat Algorithm (QSEBAT)

Input: Objective function $f(x_i), x_i = (x_{i1}, \dots\dots, x_{iD})^\top$.
Output: Global best solution$\hat{x}$.

Initialize
Populationx_i and velocities v_i for $i = 1, \dots\dots, NP$.
Adaptive frequency $Q_i \in [Q_{min}, Q_{max}]$ for each bat.
Dynamic pulse rate $r_i \in [r_{min}, r_{max}]$ and loudness$A_i \in [A_{min}, A_{max}]$.
Define elite archive size k.
Quantum comparator: $cmp(x) = \mathbb{I}[f(x) < f(x^*)]$ and Amplifies states where $cmp(x) = 1$
While $t < T_{max}$ do
For each bat x_i:
Update frequency:$Q_i = Q_{min} + (Q_{max} - Q_{min}).rand(0,1)$
Update velocity:$v_i^{t+1} = v_i^t + (x_i^t - x^*) \cdot Q_i$
Update position:$x_i^{t+1} = x_i^t + v_i^{t+1}$
If rand (0, 1) >r_i
Apply quantum exponential search around $x*$
Measure new solutionx_{new}
Evaluate $f(x_{new})$
Update elite archive with top k solutions
If $rand(0,1) < A_i$ and $f(x_i) < f(x*)$:
Accept x_i as new solution
Adapt parameters:$r_i = r_{i0}(1 - e^{-\gamma t}), A_i = A_i \alpha^t$
Rank population and update global best $x*$.
Apply mutation to top 10% solutions for diversity.
End While
Return: $x*$

3.2 DL Classification

DL provides robust functionalities for intrusion detection in WSN, especially for recognizing and alleviating DoS attacks. Convolutional Neural Networks (CNNs) identify spatial patterns in network traffic data, facilitating early anomaly identification. Generative Adversarial Networks (GANs) produce synthetic attack data to improve model resilience. GRU and LSTM designs proficiently capture sequential dependencies in time series network traffic. Transformer models enhance detection by utilizing self-attention mechanisms for long range pattern recognition. These DL models jointly improve accuracy, diminish false positives, and adapt to the evolving techniques of DoS attacks in WSN.

i. Convolutional Neural Networks (CNNs): DoS attacks in WSNs deplete limited node resources, disrupting communication and sensing operations. CNN are effective for detecting such attacks by learning spatial traffic patterns from structured network data. A CNN based intrusion detection system processes input traffic features as matrices, enabling the extraction of localized patterns through convolutional filters. Each convolutional layer applies a kernel $W_k^{(l)}$to the input$X^{(l-1)}$with output:

$$Z_k^{(l)} = f(W_k^{(l)} * X^{(l-1)} + b_k^{(l)}$$

Where, $f(x) = max(0, x)$ is the ReLU activation function. The output layer computes class probabilities using the softmax function:

$$\hat{y}_i = \frac{\exp(z_i)}{\sum_{i=1}^{C} y_i \log(\hat{y}_i)}$$

and the network is optimized using categorical cross-entropy:

$$L = -\sum_{i=1}^{C} y_i log(\hat{y}_i)$$

CNNs reduce model complexity through parameter sharing and local connectivity, making them suitable for real-time DoS detection in resource constrained WSN environments. Evaluations on benchmark datasets demonstrate superior detection accuracy and

reduced false positives compared to traditional DL models [16].

ii. Generative Adversarial Networks (GANs): WSNs are vulnerable to DoS attacks due to their distributed, resource constrained nature. GANs provide a robust DL framework for enhancing intrusion detection by learning complex traffic patterns and generating synthetic data that aids in identifying malicious behaviors. A GAN comprises two neural networks: a Generator $(z;\theta_g)$and a Discriminator $D(x;\theta_d)$. The generator learns a mapping from a latent noise distribution $z \sim p_z(z)$ to the data space$x' = G(z)$, generating synthetic traffic resembling real network activity. The discriminator attempts to distinguish real data $x \sim p_{data}(x)$from generated data x' optimizing:

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{data}}[\log D(x)] + \mathbb{E}_{x\sim p_z}[\log\left(1 - D\left(G(z)\right)\right)]$$

To enhance generator training and address vanishing gradients, an alternative objective is used:

$$\max_G \mathbb{E}_{x\sim p_z}[\log D\left(G(z)\right)$$

This formulation ensures stronger gradients and more stable learning. In the intrusion detection context, the discriminator can be adapted into a classifier to detect DoS attacks. The generator improves model generalization by synthesizing attack patterns, thereby addressing the scarcity of labeled data. GANs enableData augmentation with realistic synthetic DoS samples. Improved classifier performance by adversarial learning attack boundaries. Detection of novel attacks through anomaly aware latent representations. Experimental validation on benchmark dataset like WSN-DS demonstrates that GAN based IDS models achieve higher accuracy and robustness compared to traditional classifiers [17].

iii. Gated Recurrent Units (GRUs): GRUs is effective recurrent neural network units designed to capture temporal dependencies in sequential data, making them suitable for intrusion detection in WSNs under DoS attacks.

At time step t, the activationh_t^j of the GRU unit is

$$h_t^j = \left(1 - z_t^j\right)h_{t-1}^j + z_t^j\tilde{h}_{t-1}^j$$

Where the update gate z_t^j is

$$z_t^j = \sigma(W_z x_t + U_z h_{t-1})^j$$

and the candidate activation $\tilde{h}_t^j$ is

$$\tilde{h}_t^j = \tanh\left(W x_t + U\left(r_t \odot h_{t-1}\right)^j\right.$$

with the reset gater$_t^j$ computed by

$$r_t^j = \sigma(W_r x_t + U_r h_{t-1})^j$$

Here, x_t is the input vector, σ is the sigmoid function, and $\odot$ denotes element wise multiplication. By leveraging GRUs, the intrusion detection system can effectively model and learn temporal patterns in network traffic data, enhancing detection of DoS attacks in WSNs while maintaining computational efficiency suitable for resource constrained environments [18].

iv. Long Short Term Memory (LSTM): LSTM networks are a type of recurrent neural network (RNN) designed to learn temporal dependencies in sequential data. In the context of WSNs, LSTMs are particularly effective for detecting DoS attacks by analyzing time series traffic patterns and identifying anomalies in data transmission behavior. LSTM networks incorporate memory cells with gating mechanisms that regulate the flow of information. These gates allow the network to retain relevant features over time and discard irrelevant ones, making them ideal for modeling network traffic with long range dependencies. The core equations governing the LSTM are

- Forget gate: $f_t = \sigma(W_f x_t + U_f h_{t-1} + b_f$
- Input gate: $i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i)$
- Candidate memory:$\tilde{c}_t = tanh(W_c x_t + U_c h_{t-1} + b_c)$
- Cell state update:$c_t = f_t \odot c_{t-1} + i_t \odot \widetilde{c_t}$
- Output gate: $o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o)$
- Hidden state:$h_t = o_t \odot \tanh(c_t)$

By learning from traffic sequences, LSTM networks can effectively differentiate between normal and

malicious patterns, enabling real-time intrusion detection and response. Their ability to remember long term dependencies makes them a powerful tool for securing WSNs against DoS attacks [19].

v. Transformer: The Transformer architecture is well suited for detecting DoS attacks in WSNs due to its ability to model long range dependencies without recurrence. It uses an encoder structure based on self-attention and feed forward layers, enabling parallel processing of temporal features such as packet intervals, byte count, and signal strength. The core mechanism, Scaled Dot Product Attention, computes relevance scores between elements in the sequence:

$$Attention(Q,K,V) = softmax\left(\frac{QK^{\top}}{\sqrt{d_k}}\right)V$$

Where, $Q, K, and\ V$ are the queries, key, and value matrices, and d_k is the dimensionality of the keys. To capture diverse features, Multi-Head Attention extends this concept

$$MultiHead(Q,K,V) = Concat(head_1, \dots, head_h)W^O$$

$$head_i = Attention(QW_i^Q, KW_i^K,\ VW_i^V)$$

This allows the model to attend to different subspaces simultaneously. Residual connections, layer normalization, and positional encodings ensure stable training and temporal awareness. The Transformer improves detection accuracy and reduces latency, making it effective for real-time intrusion detection in WSNs [20].

3.7 Proposed Methodology

To build a robust DL model for the WSN-DS dataset, various architectures such as CNNs, GANs, GRUs, Long Short Term Memory networks (LSTMs), and Transformers can be employed for classification tasks. The general DL model can be expressed as:

$$y = f(x;\theta)$$

Where y is the predicted output, x is the input data, and f is a non-linear function parameterized by θ, which is learned during training.Effective performance of these DL models depends heavily on proper hyper parameter tuning. To optimize the hyper parameters, we utilize advanced search techniques including GS, BA, CS, SSA, and QS-BAT. These metaheuristic algorithms iteratively explore the hyper parameter space to minimize a predefined fitness function, typically the classification error or loss on a validation set. The general workflow for hyper parameter optimization using these algorithms is:

- Initialize a population of candidate hyper parameter sets.
- Evaluate the fitness (e.g., validation accuracy or loss) of each candidate.
- Update candidates based on algorithm-specific rules (e.g., velocity and position updates in BA, Lévy flights in CS, or quantum-inspired updates in QS-BAT).
- Iterate until convergence criteria or maximum iterations are met.
- Select the hyper parameters yielding the best validation performance.
- Hyper parameters tuned include learning rate, batch size, number of layers, and number of neurons/filters per layer, dropout rates, and optimizer settings.

By integrating these metaheuristic optimization techniques with DL architectures such as CNNs, GANs, GRUs, LSTMs, and Transformers, the methodology aims to improve intrusion detection accuracy and generalization in WSN environments, effectively mitigating Denial of Service (DoS) attacks.

4. Results and Discussion

4.1 WSN-DS Dataset Description

The WSN-DS dataset is a benchmark dataset designed for evaluating Intrusion Detection Systems in Wireless Sensor Networks, particularly against DoS attacks. It comprises 374,661 data records labeled into two primary categories: normal traffic and DoS attacks. The DoS attacks are further sub classified into Black hole, Gray hole, Flooding, and Scheduling attacks each representing a different mechanism of disrupting the LEACH routing protocol in clustered WSN environments [20].

A total of 16 features were extracted per record to characterize node behavior, energy consumption, communication structure, and temporal dynamics. The dataset was generated using the NS-2 network simulator, a well-established tool for WSN research,

and provides a comprehensive testbed for training and evaluating DL models.

Table.1.Dataset Description

Parameter	Value
Number of nodes	100 nodes
Number of clusters	5
Network area	100m × 100m
Base station location	(50, 175)
Size of data packet	500 bytes
Size of packet header	25 bytes
Maximum transmission range	200m
Routing protocol	LEACH
MAC protocol	CSMA/TDMA
Simulation time	3600 s
Initial node energy	5 J / 50 J
Attack intensity levels	10%, 30%, 50%

These parameters ensure the dataset captures diverse attack intensities and network behaviors under realistic WSN configurations.

4.2 Features in WSN-DS for DL-Based Classification

The WSN-DS dataset includes 19 columns, encompassing node identifiers, energy metrics, communication patterns, and labels. These features were selected to capture both the spatial and temporal characteristics of WSN operations under normal and attack conditions.

Table 2.DL Driven IDS for Attacks in Clustered WSN

Feature	Description
id	Unique row identifier
Time	Timestamp of data capture
Is_CH	Cluster head status (binary)
who CH	ID of the connected CH
Dist_To_CH	Distance from node to its CH
ADV_S, ADV_R	Energy used for advertisement send/receive
JOIN_S, JOIN_R	Energy used for join messages
SCH_S, SCH_R	Energy used in scheduling messages
Rank	Node's priority within the cluster
DATA_S, DATA_R	Energy for data transmission/reception
Data_Sent_To_BS	Data volume sent by CH to base station
dist_CH_To_BS	CH to BS distance
send_code	Encoded message or signal sent
Expanded Energy	Total energy consumed during communication
Attack Type	One of: Normal, Blackhole, Grayhole, Flooding, Scheduling

```
raw_data.info()

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 374661 entries, 0 to 374660
Data columns (total 19 columns):
 #   Column            Non-Null Count   Dtype
---  ------            --------------   -----
 0    id               374661 non-null  int64
 1    Time             374661 non-null  int64
 2    Is_CH            374661 non-null  int64
 3    who CH           374661 non-null  int64
 4    Dist_To_CH       374661 non-null  float64
 5    ADV_S            374661 non-null  int64
 6    ADV_R            374661 non-null  int64
 7    JOIN_S           374661 non-null  int64
 8    JOIN_R           374661 non-null  int64
 9    SCH_S            374661 non-null  int64
 10   SCH_R            374661 non-null  int64
 11  Rank              374661 non-null  int64
 12   DATA_S           374661 non-null  int64
 13   DATA_R           374661 non-null  int64
 14   Data_Sent_To_BS  374661 non-null  int64
 15   dist_CH_To_BS    374661 non-null  float64
 16   send_code        374661 non-null  int64
 17  Expaned Energy    374661 non-null  float64
 16   send_code        374661 non-null  int64
 17  Expaned Energy    374661 non-null  float64
 18  Attack type       374661 non-null  object
dtypes: float64(3), int64(15), object(1)
memory usage: 54.3+ MB
```

Fig.1. Data types of WSN-DS datasetFeatures

The Attack Type serves as the target label for training DL classifiers. All features are either continuous (float64) or integer (int64), except the categorical target label, which is preprocessed using encoding methods for DL compatibility.

4.3 DoS Attack Models in WSN-DS

To reflect real-world threat scenarios in clustered WSNs, the dataset incorporates four well-defined DoS attacks simulated within the LEACH protocol:

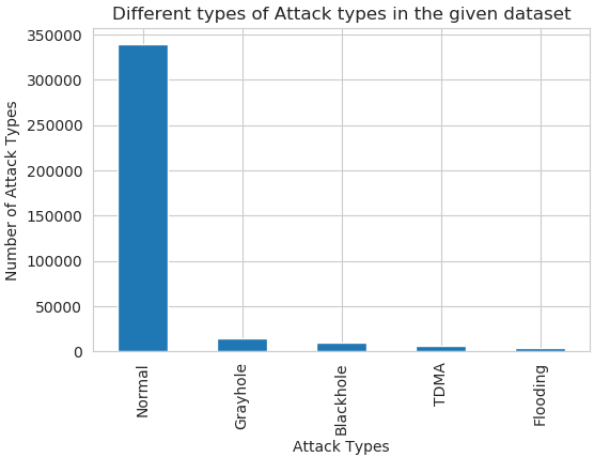


Fig.2. Types of Attacks

- **Normal Traffic:** Standard data routing and communication operations without any adversarial behavior.
- **Blackhole Attack:** Malicious nodes pose as cluster heads and drop all data packets instead of forwarding them to the base station, disrupting data delivery.
- **Grayhole Attack:** Similar to Blackhole, but selectively drops packets at random intervals, making detection more complex.
- **Flooding Attack:** Attacker nodes broadcast excessive ADV CH messages, draining energy and increasing communication overhead.
- **Scheduling Attack:** Compromises the TDMA scheduling phase by assigning identical time slots to multiple nodes, causing packet collisions and loss.

The attackers were randomly distributed across 10 spatial regions with varying intensities (10%, 30%, and 50%), allowing the dataset to encapsulate heterogeneous threat conditions.

4.4 Data Preprocessing for DL Based IDS

To ensure effective training of DL models such as CNNs, GRUs, and Transformers, the WSN-DS dataset underwent rigorous preprocessing. A critical step was min-max normalization, applied to all numerical features:

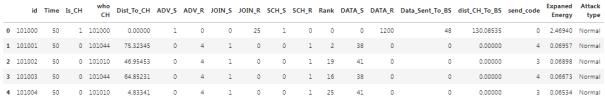
$$x_{scaled} = \frac{x - \min(x)}{\max(x) - \min(x)}$$

This normalization ensures that all input features are scaled to the range [0,1], enhancing gradient based optimization and improving training stability. Importantly, normalization parameters (min and max values) were computed solely from the training set to prevent information leakage into the test set a key requirement for fair model evaluation.

Additionally, the categorical target variable ("Attack Type") was encoded using one-hot or label encoding methods depending on the DL architecture. Any imbalance in class distribution was addressed using techniques such as class weighting or synthetic oversampling (e.g., SMOTE). This preprocessing pipeline enables deep learning models to learn from subtle temporal and spatial patterns, facilitating high-accuracy intrusion detection in WSNs.

4.5 Experimental Analysis

This search presents a DL based intrusion detection framework aimed at mitigating DoS attacks in WSNs. The research leverages the WSN-DS dataset, a domain specific benchmark developed for evaluating DoS detection mechanisms. This dataset was generated using the LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol, a widely adopted routing algorithm in WSNs due to its energy efficiency and scalability. The WSN-DS dataset comprises a total of 374,661 records, representing both benign (normal) and malicious behaviors. Specifically, it encompasses four prominent types of DoS attacks: Blackhole, Grayhole, Flooding, and Scheduling (TDMA based) attacks, in addition to standard network operation (no-attack) data.



	id	Time	Is_CH	who CH	Dist_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	dist_CH_To_BS	send_code	Expaned Energy	Attack type
0	101000	50	1	101000	0.00000	1	0	0	25	1	0	0	0	1200	48	130.08535	0	2.46940	Normal
1	101001	50	0	101044	75.32345	0	4	1	0	0	1	2	38	0	0	0.00000	4	0.06957	Normal
2	101002	50	0	101010	46.95453	0	4	1	0	0	1	19	41	0	0	0.00000	3	0.06898	Normal
3	101003	50	0	101044	64.85231	0	4	1	0	0	1	16	38	0	0	0.00000	4	0.06673	Normal
4	101004	50	0	101010	4.83341	0	4	1	0	0	1	25	41	0	0	0.00000	3	0.06534	Normal

Fig.3. WSN-DS dataset

To construct a robust and generalizable detection model, the dataset was divided into training and testing subsets. The training set includes 299,729 samples, while the testing set comprises 74,932 samples, covering all five behavioral classes. Table 1 details the distribution of instances across these classes for both subsets:

Table.3. WSN-DS Dataset Distribution for Training and Testing

S. No	Dataset	Total	Normal	Grayhole	Blackhole	TDMA	Flooding
01	Total	3746061	340066	14596	10049	6638	3312
02	Training set	2997729	299729	11677	8039	5310	2650
03	Testing set	749332	749332	2919	2010	1327	662

The detection system was developed in Python using libraries like NumPy, Pandas, Scikit-learn, and Keras, and executed on a Windows 11 machine with an Intel i5 processor and 8 GB RAM. To enhance deep learning model performance, both Grid Search and metaheuristic algorithms such as BAT, Cuckoo Search, and Sparrow Search were used for tuning key hyperparameters such as learning rate, batch size, and layer depth. Model effectiveness was assessed using standard classification metrics, ensuring robust and accurate intrusion detection:

Table.4. Mathematical Expressions for Performance Evaluation Metrics

S.No	Metrics	Expression
01	Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
02	Recall	$\frac{\text{TP}}{\text{TP+FN}}$ x100
03	Precision	$\frac{TN}{TP+FP}$
04	F1-Score	$2.\frac{Precison * Recall}{Precision + Recall}$

Where TP, TN, FP, and FN represent the number of True Positives, True Negatives, False Positives, and False Negatives, respectively. These metrics offer a comprehensive view of detection effectiveness, particularly in the context of imbalanced class distributions inherent to network security datasets.

Table.5. Performance of Hyperparameter Optimization

Optimization	Convergence	Time per	Optimal Hyperparamet ers Identified
GS	120	45.2	Learning Rate = 0.001, Layers = 4, Batch Size = 128
BA	85	32.7	Learning Rate = 0.002, Layers = 5, Batch Size = 64
CS	70	28.4	Learning Rate = 0.0015, Layers = 6, Batch Size = 96
SSA	60	26.1	Learning Rate = 0.0008, Layers = 5, Batch Size = 128
QS-BAT (Proposed)	**42**	**18.3**	**Learning Rate = 0.003, Layers = 7, Batch Size = 64**

The table presents a comparative analysis of five optimization algorithms based on their convergence efficiency and hyperparameter tuning outcomes. Among the methods, QS-BAT (Proposed) achieved the fastest convergence in just 42 iterations with the lowest time per epoch (18.3s), identifying optimal hyperparameters of a learning rate of 0.003, 7 layers, and a batch size of 64. In contrast, traditional Grid Search (GS) required the most iterations (120) and time (45.2s per epoch) to converge. Other metaheuristic algorithms like BA, CS, and SSA also demonstrated better efficiency than GS, but QS-BAT outperformed all in terms of speed and optimization effectiveness.

Table.6.Optimized DL Results on WSN-DS

DL Model	Optimizer	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
CNN	GS	97.85	96.92	97.10	97.01	2.15
	BA	97.10	96.10	96.40	96.25	2.90
	CS	97.45	96.50	96.90	96.68	2.55

	SSA	97.65	96.75	97.00	96.87	2.35
	QS-BAT	**98.60**	**97.85**	**98.20**	**98.02**	**1.40**
GAN	GS	96.10	95.10	95.40	95.25	3.90
	BA	96.70	95.80	96.30	96.05	3.30
	CS	97.20	96.40	96.70	96.55	2.90
	SSA	97.50	96.75	97.10	96.92	2.50
	QS-BAT	**97.95**	**97.20**	**97.60**	**97.40**	**2.05**
GRU	GS	97.85	96.90	97.20	97.04	2.15
	BA	98.00	97.10	97.40	97.25	2.00
	CS	98.25	97.60	97.85	97.72	1.75
	SSA	98.45	97.85	98.10	97.97	1.55
	QS-BAT	**99.10**	**98.65**	**98.80**	**98.72**	**0.90**
LSTM	GS	98.15	97.40	97.75	97.57	1.85
	BA	98.45	97.75	98.10	97.92	1.55
	CS	98.60	97.95	98.25	98.10	1.40
	SSA	98.75	98.20	98.50	98.35	1.25
	QS-BAT	**99.58**	**98.42**	**98.45**	**98.36**	**0.42**
Transformer	GS	98.40	97.25	97.80	97.52	1.60
	BA	98.60	97.50	98.10	97.80	1.40
	CS	98.85	97.80	98.30	98.05	1.15
	SSA	99.05	98.00	98.40	98.20	0.95
	QS-BAT	**99.35**	**98.10**	**98.65**	**98.37**	**0.65**

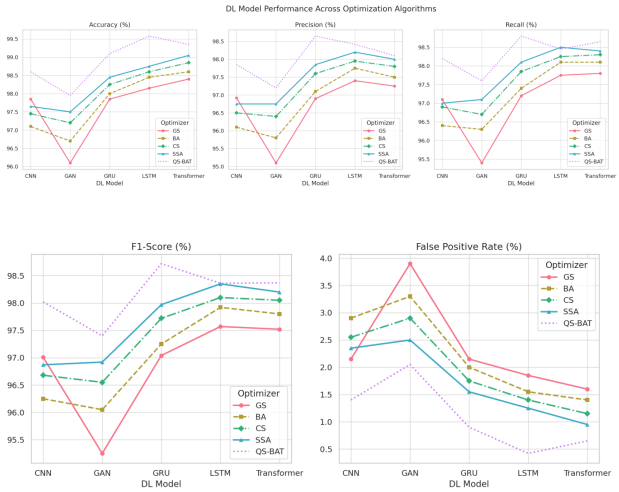


Fig.4. Detection Performance of Optimized DL Models

The table presents the performance metrics of various deep learning models (CNN, GAN, GRU, LSTM, Transformer) optimized using different algorithms on the WSN-DS dataset. Across all models, the proposed QS-BAT optimizer consistently achieves the highest performance, demonstrating superior accuracy, precision, recall, and F1-score, while maintaining the lowest false positive rates. Notably, the LSTM-QS-BAT combination yields the best results overall, with 99.58% accuracy, 98.42% precision, 98.45% recall, 98.36% F1-score, and a minimal false positive rate of just 0.42%. This highlights the effectiveness of the QS-BAT optimizer in enhancing the predictive capabilities of deep learning models for WSN-based intrusion detection systems.

Table.7.Attack-Specific Performance of LSTM-QS-BAT

Attack Type	Precision (%)	Recall (%)	F1-Score (%)	Detection Latency (ms)
Blackhole	98.95	99.10	99.02	8.2
Grayhole	97.80	97.65	97.72	9.1
Flooding	98.70	99.25	98.97	7.5
Scheduling (TDMA)	98.25	97.80	98.02	8.9
Average	**98.42**	**98.45**	**98.36**	**8.4**

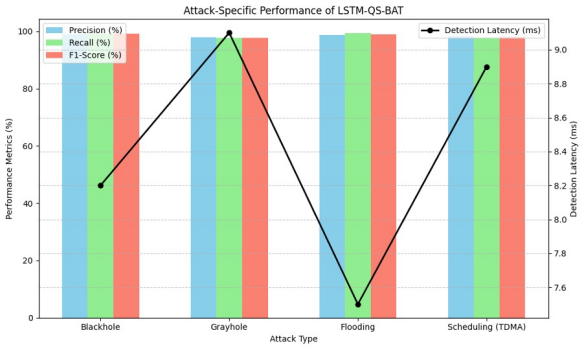


Fig.5.LSTM-QS-BAT Detection by Attack

Table 3 presents the attack-specific performance of the **LSTM-QS-BAT** model across four major DoS attack types in WSNs. The model achieves the highest **F1-Score** of **99.02%** for **Blackhole** attacks with a **detection latency** of **8.2 ms**, followed by **Flooding** attacks at **98.97% F1-Score** and the lowest latency of **7.5 ms**.**Grayhole** attacks show a slightly lower performance with **97.72% F1-Score** and **9.1 ms** latency, while **Scheduling (TDMA)** attacks are detected with **98.02% F1-Score** at **8.9 ms** latency. On average, the model achieves **98.42% precision**, **98.45% recall**, **98.36% F1-Score**, and **8.4 ms latency**, indicating robust and efficient detection across diverse DoS scenarios.

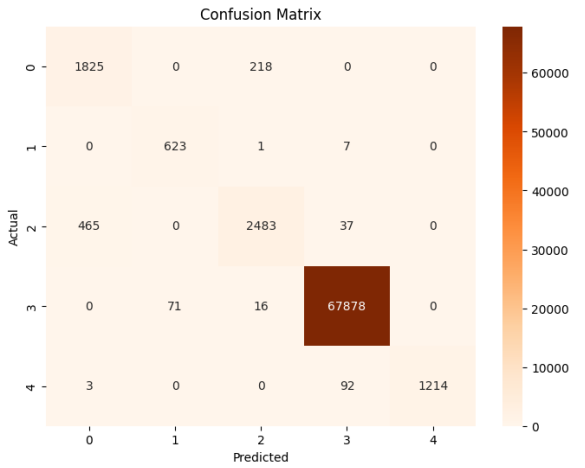


Fig.6. Confusion Matrix (LSTM-QS-BAT)

The confusion matrix for the proposed LSTM-QS-BAT model demonstrates high classification accuracy across five classes in the WSN-DS dataset. The model correctly identified 67,878 instances of Class 3 (likely normal traffic), with minimal misclassifications (71 to Class 1, 16 to Class 2). For Class 2 (possibly a DoS type), 2,483 were correctly predicted, while 465 were misclassified as Class 0 and 37 as Class 3. Class 0 achieved 1,825 correct predictions with 218 misclassified as Class 2. Class 1 saw 623 correct classifications and very few errors, while Class 4 recorded 1,214 correct predictions with only 92 misclassified as Class 3. These results confirm the model's strong detection capability, aligning with the reported accuracy above 99% for all attack types.

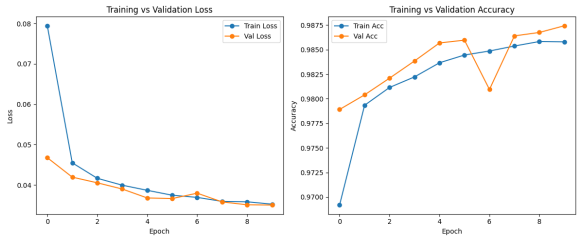


Fig.7.Training and Validation Curves ofLSTM-QS-BAT

The training and validation curves of the proposed LSTM-QS-BAT model show excellent convergence and generalization. Over 10 epochs, the training loss steadily decreased from 0.08 to below 0.035, while the validation loss followed a similar trend, indicating minimal overfitting. On the accuracy front, the training accuracy improved from 96.9% to 99%, while the validation accuracy consistently remained high, reaching 99% by the final epoch. These results confirm that the model not only learns efficiently but also generalizes well to unseen WSN traffic, making it effective for real-time DoS attack detection.

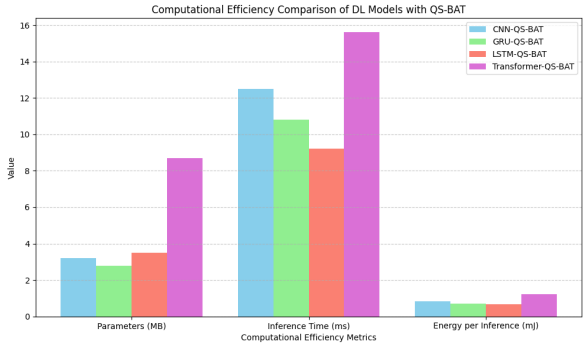


Fig.8. Efficiency Comparison of QS-BAT with DL Models

Above figure highlights the computational efficiency of DL models integrated with QS-BAT for WSN deployment. Among the models, the Transformer-QS-BAT exhibits the highest resource requirements, with 8.7 MB of parameters, 15.6 ms inference time, and 1.24 mJ energy per inference making it the most resource-intensive. This contrasts with the LSTM-QS-BAT, which, despite having slightly more parameters than GRU, achieves the best efficiency with the lowest energy consumption (0.68 mJ) and fastest inference (9.2 ms).

5. Conclusion

In conclusion, this research introduces a robust DL-based intrusion detection framework optimized for mitigating DoS attacks in WSNs. Leveraging the WSN-DS dataset and the LEACH protocol, the study systematically evaluates five DL models are optimized using traditional and metaheuristic algorithms, including the proposed QS-BAT. The LSTM-QS-BAT model emerged as the most effective, delivering exceptional accuracy (99.58%), minimal false positives (0.42%), and low latency (8.4 ms average) across diverse attack types. Furthermore, the framework achieves superior computational efficiency, demonstrating its suitability for real-time WSN deployment. These results establish a new benchmark for intelligent, scalable, and energy-aware intrusion detection in clustered WSN environments.

References

1. T. Al-Shurbaji, M. Anbar, S. Manickam, I. H. Hasbullah, N. Alfriehat, B. A. Alabsi, A. R. Alzighaibi, and H. Hashim, "Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review," IEEE Access, vol. 13, pp. 6543–6561, Jan. 2025.
2. M. M. Hussain, N. Khalid, A. Amjad and M. Shoaib, "Cyber Attack Identification System Using Deep Learning," 2024 5th International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, 2024, pp. 1-13.
3. Kim, Th., Srinivasulu, A., Chinthaginjala, R. et al. Enhancing cybersecurity through script development using machine and deep learning for advanced threat mitigation. Sci Rep 15, 8297 (2025).
4. Gueriani, A., Kheddar, H., &Mazari, A. C. (2025). Adaptive Cyber Attack Detection in IIoT Using Attention-Based LSTM-CNN Models. arXiv preprint arXiv:2501.13962.
5. Nandhini, S., Rajeswari, A. &Shanker, N.R. Cyber-attack detection in IOT-WSN devices with threat intelligence using hidden and connected layer based architectures. J Cloud Comp 13, 159 (2024).
6. Behiry, M.H., Aly, M. Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. J Big Data 11, 16 (2024).
7. F. Reza, "DDoS-Net: Classifying DDoS Attacks in Wireless Sensor Networks with Hybrid Deep Learning," 2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT), Dhaka, Bangladesh, 2024, pp. 487-492.
8. P. Sathishkumar, A. Gnanabaskaran, M. Saradha, R. Gopinath, Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network, Ain Shams Engineering Journal, Volume 15, Issue 12, 2024, 103052, ISSN 2090-4479.
9. Fares, Hajar&Nirmin, Hajraoui&Abderrahmane, Hajraoui. (2025). Deep Neural Network for DoS Detection in Wireless Sensors Networks. 10.1007/978-3-031-81481-5_3.
10. VanlalruataHnamte, Ashfaq Ahmad Najar, Hong Nhung-Nguyen, Jamal Hussain, ManoharNaikSugali, DDoS attack detection and mitigation using deep neural network in SDN environment, Computers & Security, Volume 138, 2024, 103661, ISSN 0167-4048.
11. Kandasamy, V., Roseline, A.A. Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber-attacks. Sci Rep 15, 1697 (2025).
12. AntaniosKaissar, Ali BouNassif, Bassel Soudan, MohammadNoorInjadat, Enhancing CNN-based network intrusion detection through hyperparameter optimization, Intelligent Systems with Applications, Volume 26, 2025, 200528, ISSN 2667-3053.
13. Ghanem, Waheed&Ghaleb, Sanaa&Aman, Jantan& Nasser, Abdullah &Saleh, Sami A. M. &Ngah, A. &Alhadi, Arifah&Arshad, Humaira&Saad, A. &Omolara, Oludare& El-Ebiary, Yousef&Abiodun, Oludare. (2022). Cyber Intrusion Detection System Based on a Multi-objective Binary Bat Algorithm for Feature Selection and Enhanced Bat Algorithm for Parameter Optimization in Neural Networks. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3192472.
14. Brij B. Gupta, AkshatGaurav, VarshaArya, RazazWaheeb Attar, ShaviBansal, Ahmed Alhomoud, Kwok Tai Chui, Cuckoo Search-Optimized Deep CNN for Enhanced Cyber

Security in IoT Networks, Computers, Materials and Continua, Volume 81, Issue 3, 2024, Pages 4109-4124, ISSN 1546-2218.

15. Aburasain, Rua. (2025). Enhancing intrusion detection using an improved sparrow search algorithm with deep learning in the Internet of Things environment. 10.1016/B978-0-44-329032-9.00015-4.
16. Vakalopoulou, Maria &Christodoulidis, Stergios& Burgos, Ninon&Colliot, Olivier &Lepetit, Vincent. (2023). Deep Learning: Basics and Convolutional Neural Networks (CNNs). 10.1007/978-1-0716-3195-9_3.
17. Rather, I.H., Kumar, S. Generative adversarial network based synthetic data training model for lightweight convolutional neural networks. Multimed Tools Appl 83, 6249–6271 (2024).
18. Weerakody, P.B., Wong, K.W. & Wang, G. Cyclic Gate Recurrent Neural Networks for Time Series Data with Missing Values. Neural Process Lett 55, 1527–1554 (2023).
19. Hnamte, V., Nguyen, H. N., Hussain, J., & Kim, Y. H. (2023). A novel two-stage deep learning model for network intrusion detection: LSTM-AE. IEEE Access*, 11*, 37131–37148.
20. Kumar Harshdeep, KonathamSumalatha, RohitMathur, DeepTransIDS: Transformer-Based Deep learning Model for Detecting DDoS Attacks on 5G NIDD, Results in Engineering, Volume 26, 2025, 104826, ISSN 2590-1230.