International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/38 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE

Enhancing DDoS Detection and Mitigation in 5G Networks Using LSTM and Harris Hawk Optimization

Sharma Ji
Department of Computer Science and Engineering, IFTM University, Lodhipur Rajput, Moradabad, Uttar Pradesh, India.
✉ saurabh12d@gmail.com

Abhishek Mishra
Department of Computer Science and Engineering, IFTM University, Lodhipur Rajput, Moradabad, Uttar Pradesh, India.
abhimishra2@gmail.com

Received: 26 May 2025 / Revised: 01 August 2025 / Accepted: 17 August 2025 / Published: 30 August 2025

Abstract – High-demand services like autonomous factories and smart cities depend on 5G networks, but they also present security risks like Distributed Denial of Service (DDoS) attacks. These attacks reduce the viability of conventional detection and mitigation techniques by interfering with network resources, interfering with communication, and compromising system dependability. In order to identify and neutralize DDoS assaults, this study proposes an intelligent and adaptable system that can include Harris Hawk Optimization (HHO) and Long Short-Term Memory (LSTM). While the HHO algorithm is used to fine-tune the mitigation approach dynamically and narrow down the model parameters, LSTM may learn the temporal traffic patterns and, as a result, accurately identify DDoS activity. Additionally, the Fox-style Optimization Algorithm is used to reroute traffic to trusted and energy-efficient nodes when an attack has been detected. By giving priority to trust value, energy level, and network speed, this algorithm reduces the amount of disturbance to the service. The effectiveness of the proposed framework is demonstrated experimentally with a 95.63% detection rate, 94.56% specificity, 95.02% sensitivity, and 94.45% accuracy. Additionally, with a margin of improvement of 5.4%, 7.3%, 33.8%, and 11.5%, respectively, the Harris Hawk Optimization strategy outperforms other optimization strategies such as DSO, EVO, GFROA, and PCOA. Through reliable, low-latency communication even during attacks, the framework not only improves the security posture of 5G networks but also boosts their performance.

Index Terms – 5G Networks, DDoS Detection, DDoS Mitigation Long Short-Term Memory (LSTM), Harris Hawk Optimization (HHO), Optimization Strategies, Smart Infrastructure Security.

1. INTRODUCTION

The fifth-generation (5G) mobile networks will offer previously unheard-of benefits, such as ultra-high data speeds with low latency, the ability to connect to a large number of devices, and enhanced spectral efficiency capabilities. This represents a paradigm shift in wireless communication. 5G is now the foundation of modern digital infrastructure as these advancements have made high-impact applications like telemedicine, intelligent manufacturing, autonomous driving, and smart cities the standard [1]. However, 5G also brings with it a more dispersed and complicated regime that is linked to much more potent and extensive dangers. Among the most important are Distributed Denial of Service (DDoS) attacks, which can cause network traffic congestion to the point that the network can no longer function [2].

We observe that the ultra-dense device connections, dynamic network slicing, and virtualized infrastructure in the 5G environment make it more susceptible to DDoS attacks than the traditional network. Because DDoS assaults are so dynamic and ever-evolving, it is difficult for traditional security systems to recognize novel or sophisticated attack techniques in real time [3]. This has made it necessary to have astute, quick-thinking, and predictive techniques in order to recognize and stop these dangers as soon as possible and with high accuracy.

Machine learning, particularly deep learning techniques, was found to be an efficient intrusion detection method to address this. Among them, the Long Short-Term Memory (LSTM) networks a subset of Recurrent Neural Networks (RNN) have proven to be highly effective in learning temporal dependencies and uncovering hidden patterns in sequential data, such as network traffic [4]. LSTM networks provide the timely and appropriate use of traffic dynamic features, enabling the identification and execution of DDoS behaviors

RESEARCH ARTICLE

before they eventually result in significant issues with service delivery. However, this is insufficient to recognize it. In order to keep the network robust and functional, mitigation techniques are also essential. This necessitates the development of intelligent routing systems that can separate the network's vulnerable nodes, swiftly adjust to changing network conditions, and redirect traffic in a secure manner. The Harris Hawk Optimization (HHO) algorithm offers a novel approach to routing decision optimization in a dynamic environment, based on the strategic searching behavior of Harris hawks [5]. Additionally, by considering a crucial set of parameters, namely trust value, energy consumption, and throughput, Fox Inspired Optimization Algorithm (FIOA) will ensure both an energy-efficient and trust-aware routing [6].

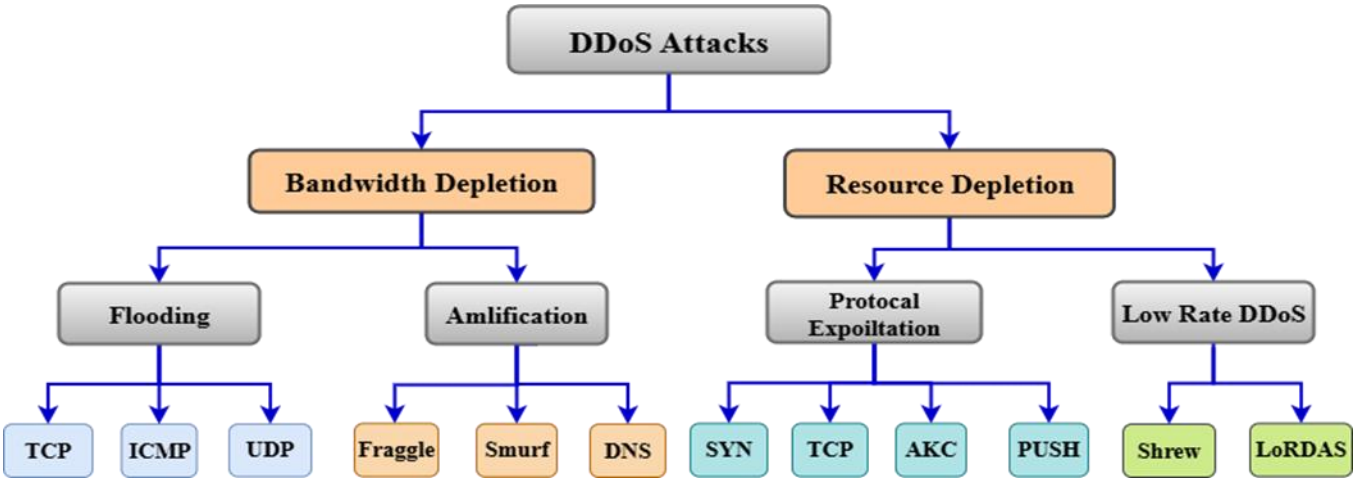


Figure 1 Classification of DDoS Attacks

In order to maximize the security and performance of 5G networks, the paper's suggested (hybrid) framework uses LSTM-based DDoS detection in conjunction with HHO and FIOA-based routing optimization. Even when threats are ongoing, the suggested system will maintain communication, enhance reactions, and stop real-time attacks [7]. The established experimental validation demonstrates significant improvements in detection accuracy and routing efficiency when compared to outdated methods, demonstrating the framework's suitability as a solution for next-generation wireless network security [8].

To identify DDoS assaults in 5G networks, researchers have used deep learning and machine learning techniques. However, choosing the appropriate features for training and testing models is a constant issue since feature selection is essential to improving detection efficiency. Detection is effective by virtue of packet feature engineering due to the fact that it facilitates the easy discovery of meaningful patterns in the raw network data. In order to handle security threats like phishing and DDoS attacks, adaptive machine learning algorithms like the following algorithms have been used: Support Vector Machine (SVM), Random Forest (RF), Logistic Regression (LR), K-Nearest Neighbors (KNN), and Gaussian Naive Bayes (GNB). Due to its ability to preserve temporal dependencies, LSTM networks are utilized to identify DDoS assaults; nonetheless, a comprehensive solution for mitigating DDoS attacks under 5G overlay networks remains a research gap.

In order to overcome existing system constraints, the study suggests a strong, clever architecture for identifying and preventing DDoS in 5G networks.

- In order to improve data security and communication effectiveness, the project intends to develop a revolutionary deep learning method for identifying and thwarting DDoS assaults in 5G networks.
- By precisely identifying DDoS assaults and lowering false alarms, the ACLSTM paradigm is being used to improve network security and Quality of Service.
- For secure data transmission in 5G networks, the ACLSTM model is optimized using the Harris Hawks Optimization method, integrating trust-aware and energy-efficient routing with the Fox Inspired Optimization method.

The research work’s contribution the following is an outline of the innovative advanced approaches’ goals.

- For the safe administration of 5G networks, the paper suggests a hybrid architecture that combines optimization methods like HHO and FIOA with LSTM-based DDoS detection.
- The ACLSTM model was created to reduce false positive rates and improve attack detection accuracy.
- In order to improve model responsiveness, the strategy incorporates intelligent routing based on trust, energy, and

RESEARCH ARTICLE

throughput using a Human-Handled Optimization (HHO) approach.

- To guarantee reliable and secure communication even in the face of persistent assaults, the FIOA algorithm is being combined with trust-aware and energy-efficient routing.
- When compared to traditional techniques, the experimental validation showed notable improvements in routing efficiency and detection accuracy.

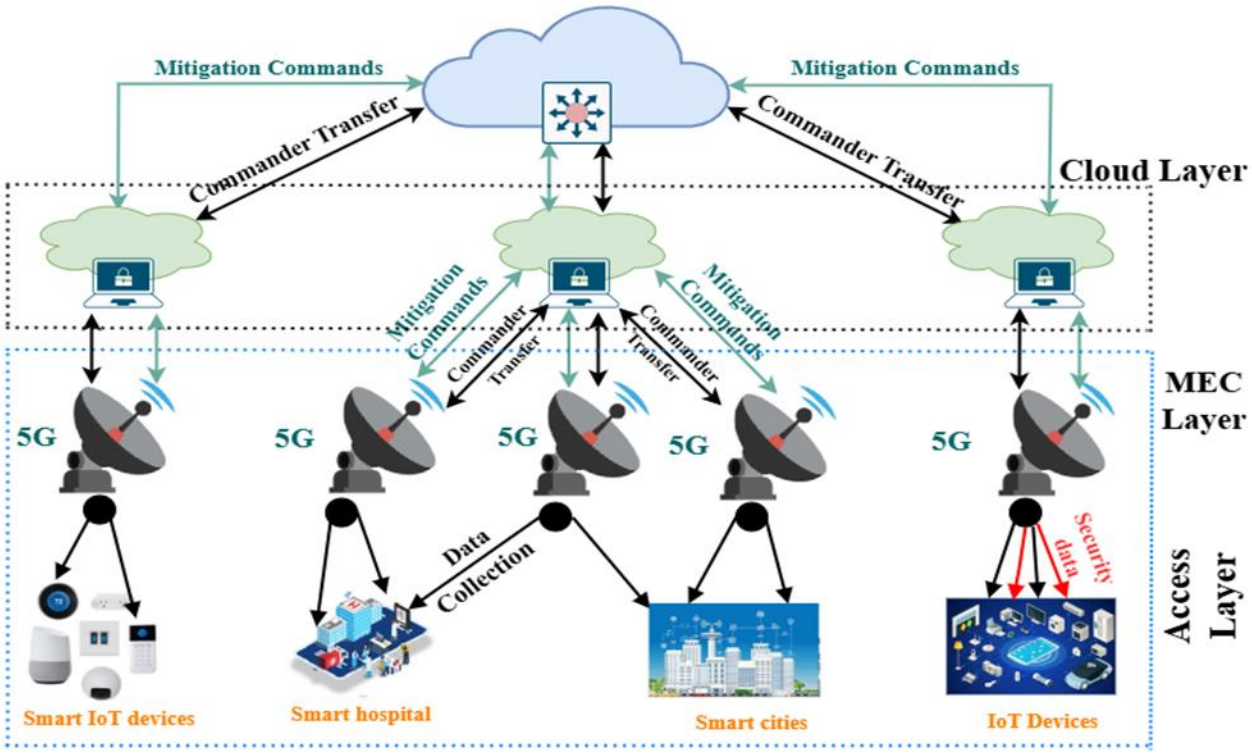


Figure 2 An Overview of the Architecture of an IoT System Enabled by 5G

The suggested method for identifying and preventing DDoS assaults in 5G networks is thoroughly assessed in the sections that follow. In Section 2, the relevant literature is reviewed, with a focus on the latest advancements in DDoS detection and prevention techniques in the context of 5G network development. The suggested approach, which includes an explanation of the system and the operating structure, is introduced in section 3. The Adaptive Cascaded LSTM employing HHO is shown in Section 4, along with the methods that enable successful attack detection. The use of optimal routing, its goal function, and associated limitations are examined in section 5 in order to reduce the attack's impact. The outcomes of the analytical and simulation models are given in section 6. The report concludes in section 7, with significant results and opportunities for further research.

2. RELATED WORK

Increasing the effectiveness of DDoS detection systems has been made possible in large part by optimization techniques. In order to enhance model performance, recent research has added optimization strategies inspired by nature. For example, Singh et al. [9] in (2024) improved detection time by 20% by combining an LSTM model with the Grey Wolf Optimization (GWO) technique. An innovative method is the Fox Inspired Optimization (FIO) technique, which uses foxes' adaptive hunting behavior to adjust deep learning models' hyperparameters for improved detection accuracy.

Although DDoS detection has advanced, several issues still require attention. Increasing processing costs, changing assault methods, and the requirement for real-time detection remain major obstacles. In order to overcome these issues, researchers such as Ahmed et al. [10] in (2024) have emphasized the role of adaptive learning models and light-weight cryptography techniques. These limitations can be bridged by coupling LSTM with the Fox-Inspired Optimization approach, which presents a more accurate, efficient, and dynamic detection mechanism.

A concurrent, closed-loop self-sustaining architecture utilizing 5G/6G networks for providing self-protection services against DDoS attacks was proposed by Caballero et al. [11] in 2023. The architecture evaluated DSPs and ISPs'

RESEARCH ARTICLE

functions across various areas for enhancing the performance of the services. The architecture was extensively tested to ensure accurate evaluation and verification of this concept, implementation, and effectiveness of the architecture. By reviewing potential risks, the proposed distributed system was examined in various fields, enhancing system efficiency and network security as a whole.

Khedr et al. [12] presented FMDADM, a five-layer architecture based on SDN that is intended for DDoS detection and mitigation, in 2023. The framework consists of four separate modules, the first of which starts early threat detection by using a 32-packet window. Preprocessing, feature extraction, model training/testing, and attack categorization are the four main steps in the machine learning-based detection technique. In order to distinguish between benign and malevolent behavior, FMDADM efficiently examines both high-rate and low-rate traffic patterns. Threat mitigation is the main emphasis of the last phase, which guarantees a precise and prompt reaction. The model's ability to enhance network security in dynamic conditions was shown by extensive performance assessments. The framework is a viable option for real-time DDoS attack detection and mitigation due to its accuracy and versatility.

Jmal et al. conducted a comprehensive examination of several approaches for identifying and stopping DDoS assaults on IoT devices [13]. The research investigated the usage of blockchain, Software-Defined Networking (SDN), and predictive modeling for improved detection capabilities. The proposed method employed blockchain technology to improve the detection and mitigation process and secure the system through the integration of a secure IoT system with many controllers and SDN.

A fog computing-based mitigation solution was proposed by Lawal et al. [14] in 2022 to enhance detection and response against DDoS attacks. The approach was designed to handle resource constraints that are often encountered in networked environments. Based on anomaly detection techniques, the scheme employed a k-Nearest Neighbors (KNN) model to identify malicious activity. Employing a shared database, anomaly detection helped to distinguish malicious activity from normal traffic patterns. In addition, by correlating incoming traffic to a database of pre-determined signatures, a signature-based detection system was included to recognize well-known patterns of attacks. The combo method increased the accuracy and efficacy of DDoS attack detection while reducing false positives.

An intrusion detection system (IDS) based on deep autoencoders was created by Ahmed et al. [15] in 2022 to detect hostile activities in real-time situations. By using an LSTM autoencoder architecture, the model was created to identify intrusive threats in Industrial Internet Control Systems (IICS). With a standard dataset, its performance was evaluated by comparing it with other existing methods to enhance questionable activity detection. To enhance security within IoT networks, Ahmed et al. [16] applied the Federated-Simple Recurrent Units (SRUs) paradigm in 2022. The improved SRU architecture was designed to rectify gradient vanishing issues and reduce computing costs. The technique enhanced intrusion detection system (IDS) privacy preservation by enabling effective inter-network communication among multiple ICS networks. To evaluate the overall efficacy and performance of the model, simulation tests were performed.

Table 1 Comparative Analysis of Various Methods Discussed in the Literature Review

Authors	Technique	Key Contribution	Advantage	Disadvantage	Dataset
Singh et al. [9]	Grey Wolf Optimization (GWO) with LSTM	20% faster detection time using LSTM and GWO	High accuracy Faster detection	Sensitive to parameter tuning	Not stated
Ahmed et al. [10]	FIO (Fox-Inspired Optimization) plus LSTM	Adaptive detection model that combines FIO and LSTM to increase accuracy and save costs	Dynamic adaptation Reduced processing cost	Computational complexity	Not stated
Caballero et al.[11]	Distributed Architecture with Closed Loops	Self-sustaining DDoS defense architecture in 5G/6G utilizing DSP/ISP cooperation	Distributed protection Real-time response	Complex to implement across multiple providers	Not stated

RESEARCH ARTICLE

Khedr et al. [12]	SDN + ML Framework, or FMDADM	Five-layer machine learning architecture with mitigation, feature extraction, and early detection	Handles high/low-rate traffic Early detection	Not tested on public datasets	Not stated
M. Sharma et al. [13][14]	Naive Bayes+ K-Nearest Neighbors	DDoS detection on network logs using resampling and multiple classifiers	Simple and interpretable	Lower accuracy on complex data	Custom DDoS dataset
A. K. Verma et al. [15][16]	Multi-Level IoT Mitigation (REATO)	Edge-fog-cloud framework (NOS middleware) for real-time attack prevention	Real-time detection Scalable architecture	Needs specialized middleware	NOS Middleware
Arshi et al. [17]	Composite MLP Framework	MLP with efficient feature extraction for B5G networks	Good generalization	May overfit without proper regularization	5G network dataset
Almiani et al.[18]	Kalman + BPNN	Deep Kalman BPNN for DDoS detection in 5G IoT	Improved accuracy Supports time-series data	Computationally intensive	CICDDoS2019
Kim et al. [19]	Feature Selection + ML	IoT DDoS detection with optimized features in 5G core networks	Reduced dimensionality Improved speed	Feature selection quality-dependent	Not specified
Sharafaldin et al. [20][21]	Dataset Development (CICDDoS2019)	Realistic dataset and taxonomy for DDoS; evaluates modern vs. legacy networks	Comprehensive benchmark	Lacks recent attack types	NSL-KDD, CICIDS2017

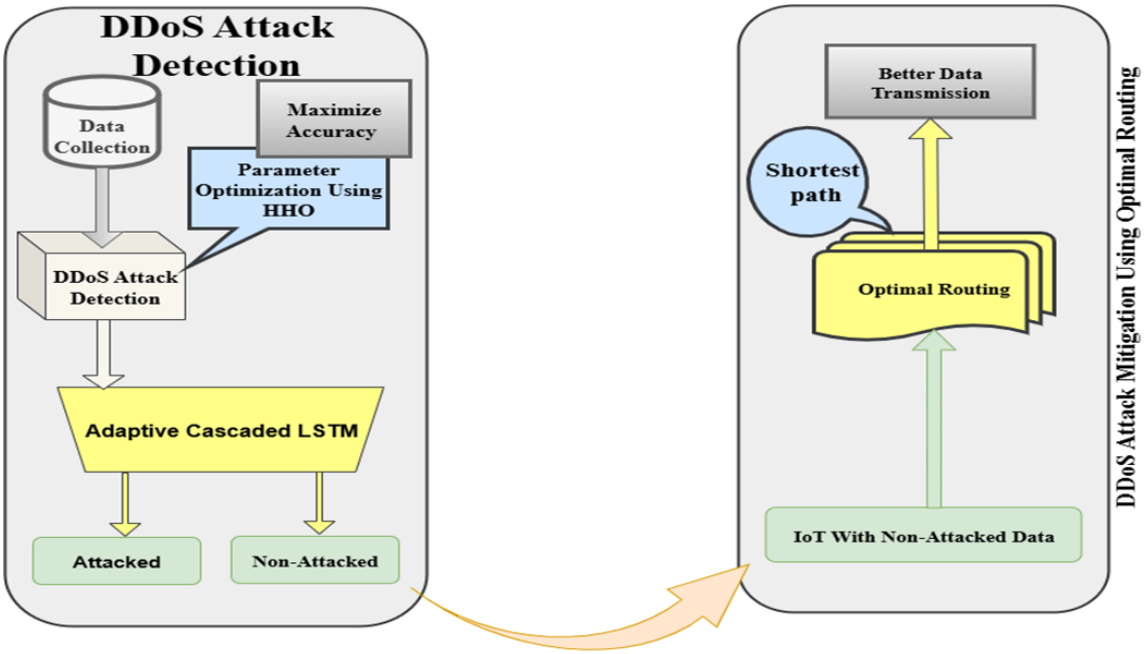


Figure 3 An Overview of the Architecture of an IoT System Enabled by 5G

RESEARCH ARTICLE

An autoencoder-based detection method that combines convolutional and recurrent networks was suggested by Ahmed et al.[17] in 2022 to identify cyberthreats in IoT networks. The Sliding Window (SW) method was utilized for feature extraction to better learn latent representations. In addition, fully connected layers were utilized to enhance classification performance for assault events by identifying temporal as well as spatial data. The proposed paradigm worked well in real IIoT networks, based on empirical results. Singh et al. [18] explored advanced deep learning models for identifying DDoS attacks in 2022. Researchers from various disciplines studied the distinctive attributes of DDoS attacks, altering a number of methodologies for a comprehensive evaluation. For the purpose of enhancing detection effectiveness, the research also confirmed several performance measures along with protection mechanisms. In an effort to enhance accuracy and reduce computational expense, Mishra et al. [19]employed an ensemble classifier based on majority voting in 2022. The model demonstrated better performance when tested using the CICDDoS2019 dataset. Experimental results supported the enhanced DDoS detection accuracy of the proposed method.

Application of variational autoencoders (VAEs) as a basic component of an intelligent security system to discriminate between malicious and genuine communications was explored by Barli et al. [20] in 2021. To ensure accurate detection, they employed a two-stage process. The VAE model generated latent encodings during the first step, capturing significant feature representations. These representations were analyzed to detect anomalies in the second stage. The research highlighted the advantage of VAEs over traditional encoders in that they prevent overfitting since they encode inputs along a latent space rather than compressing them into a point. This characteristic allowed the model to generalize sufficiently even when presented with unusual or radically different network traffic patterns. The efficiency of the suggested VAE-based technique in enhancing anomaly detection and fortifying overall network security was demonstrated by the evaluation of its performance on two datasets. In 2021, Mishra et al. [21] developed a security framework for detecting DDoS attacks and tested how well it distinguished between DDoS traffic and normal traffic at minimal computational cost using a number of entropy variations. Through its ability to reduce the severity of attacks, this technique enhanced overall network security.

This Table 1, highlights the key points of the latest research on methods of detecting DDoS attacks. Multiple innovative techniques are on view, such as LSTM and GWO or FIO optimization. The study looks into advances in fog computing, SDN-based architecture, using blockchain, and adaptive learning. All of these strategies focus on resolving important matters such as system efficiency, quick response in real time, and reliable detection.

2.1. Problem Statement

5G networks, which provide fast wireless connection, have also advanced significantly in tandem with the Internet of Things' explosive expansion. However, DDoS assaults have increased as a result of the growth of 5G-enabled IoT networks, which can negatively affect network availability and impair CPU performance. Time and energy usage are further increased by inefficient data transmission pathways. Consequently, several researchers have created methods to identify DDoS assaults. Notwithstanding these developments, there are still certain issues with current methods, which are listed below:

- The majority of current methods mainly concentrate on identifying DDoS assaults, but they are unable to mitigate the impacted nodes, which causes the data transmission process to be disrupted. The suggested approach effectively identifies and mitigates DDoS-attacked nodes in order to solve this problem, guaranteeing that 5G-enabled IoT networks experience the least amount of latency possible.
- Large and complicated datasets are difficult for current models to handle effectively. Nevertheless, the suggested model makes use of a cascaded deep learning approach, which facilitates the efficient processing and management of extremely complex and large datasets.
- Previous models for detecting DDoS attacks in 5G-enabled IoT networks had several drawbacks, including lengthy training times, high processing times, and expensive prices. By employing a sophisticated conventional method, the suggested model gets over these drawbacks and guarantees quicker and more effective identification.
- After identifying DDoS-attacked nodes, current techniques are unable to guarantee quick and safe data transfer. In order to solve this, the suggested model chooses the most effective route for safe and smooth network data transport.
- In 5G-enabled IoT networks, previous DDoS attack detection algorithms frequently experience latency and poor performance. The suggested method ensures dependable and effective performance by lowering energy consumption and increasing network trust and throughput.

The DDoS attack detection system incorporates a deep learning approach to overcome these shortcomings, hence reducing its shortcomings. By optimizing IoT-based data gathering, the suggested technique improves training and fixes intricate model problems. To ensure effective and delay-free data connection, an innovative optimization method is also used to choose the best routing path. The delay analysis

RESEARCH ARTICLE

verifies that, within a certain time period, the planned model accomplishes dependable and quick data transport.

3. PROPOSED METHOD

3.1. Overview of the Architecture for An Iot System With 5G Support

As shown in Figure 2, the three primary levels of the proposed 5G IoT architecture are the Access Layer, Multi-access Edge Computing (MEC) Layer, and Cloud Layer. These layers are all essential to establishing safe and instantaneous communication. Physical components like as servers, wireless devices, and access points are included in the access layer. These elements support the generation and transmission of data through IoT devices in several domains, including hospitals and smart cities. The acquired information is sent to the MEC [22] Layer, which facilitates real-time data processing and reduces latency. Additionally, this layer uses intelligent gateways to enable device networking and connection routing for control signals.

The MEC Layer computes received information locally, transfers processing to the cloud, and identifies potential security risks at an edge. It is essential for carrying out appropriate mitigation measures and issuing orders for additional processing. Despite its advantages, this layer is still vulnerable to cyberattacks that might result in data loss or utility loss [23]. The Cloud Layer serves as the primary processing hub for evaluating global threats and enforcing mitigation actions. It also provides robust isolation measures for widespread data protection.

To improve real-time performance, resilience, and immunity, the proposed system distributes both detection and mitigation functions at MEC and Cloud Layers, in contrast to traditional architectures where detection is typically centralized. Such a tiered philosophy, which is inappropriate in the old models, reduces the time it takes to identify an attack, avoids resource waste, and permits secure data routing.

3.2. A Robust Methodology for Identifying and Preventing DDoS Attacks

To provide a global DDoS detection and mitigation technique, the proposed system integrates Adaptive Cascaded Long Short-Term Memory (ACLSTM), Harris Hawks Optimization [24], and optimal routing algorithms as shown in Figure 3. There are two significant phases to the framework:

Phase of Detection: The NIPS gathers and monitors data by spotting anomalous patterns. The ACLSTM model's hyperparameters are automatically optimized using the HHO algorithm, improving adaptability to shifting traffic patterns. Optimized ACLSTM model then gives benign or malicious categorization to a network traffic on the basis of the learnt temporal patterns in order to precisely detect DDoS threats.

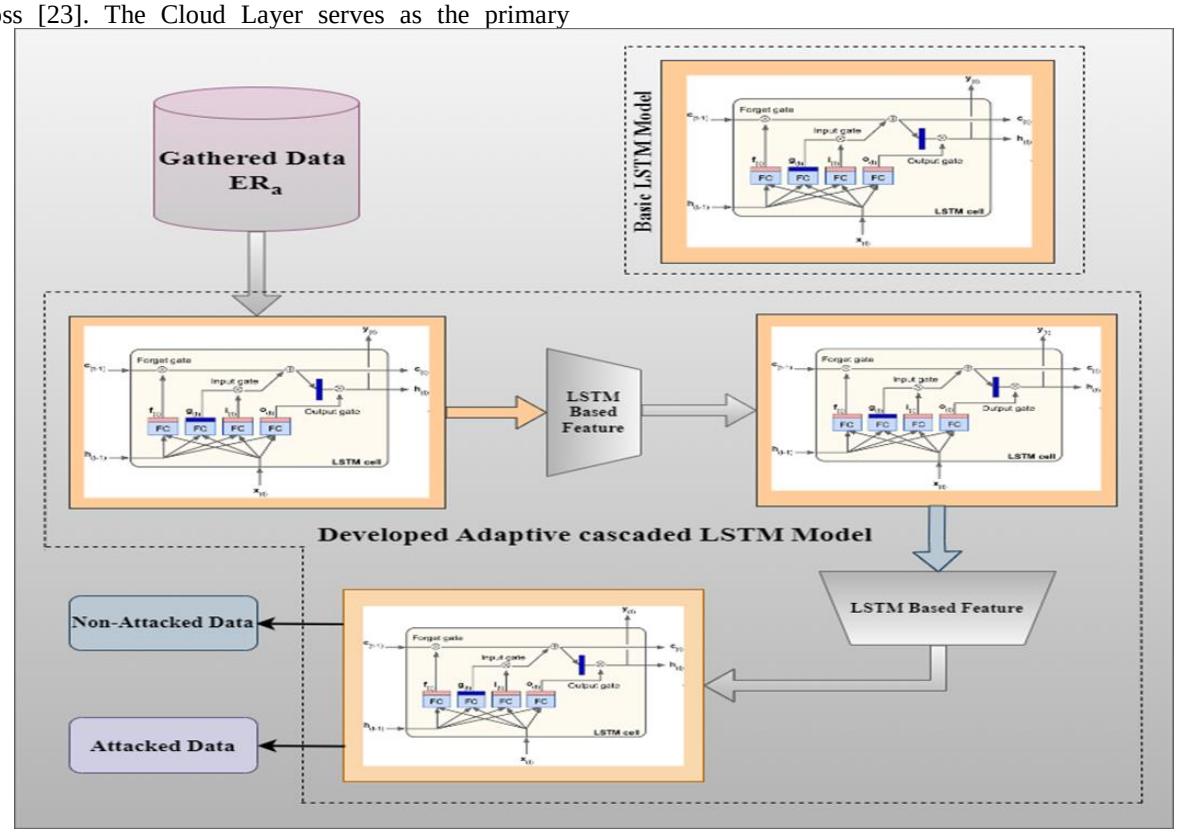


Figure 4 Proposed View of the Suggested Adaptive Cascaded ACLSTM for Detection

RESEARCH ARTICLE

Phase of Mitigation: The system ensures that only clean data reaches its intended recipient and stops harmful traffic as soon as malicious behavior is identified. By identifying the most secure and effective transmission routes, the optimal routing module one that adheres to the shortest-path concepts reduces delays or even makes use of faulty network portions. In several ways, the provided technique differs from the earlier models:

In contrast to single layer-based LSTM techniques, it suggests a cascaded LSTM architecture that enables a deeper learning of complicated attack patterns. The detection accuracy and system responsiveness to evolving attack scenarios are significantly enhanced by the use of HHO in parameter optimization.

Since most existing methods are limited to detection, this system's real-time mitigation, which incorporates intelligent routing, ensures that service will continue to function even in the event of an attack.

A comprehensive end-to-end solution for safe data transmission in the Internet of Things environment, spurred by 5G, will be provided by the confluence of routing intelligence and adaptive learning.

Overall, the architecture improves detection accuracy, reduces false positives, and makes it easier to interpret data streams while implementing a strong and scalable protection against sophisticated DDoS attacks.

3.3. DDoS Data Collection

The Canadian Institute for Cybersecurity created the CICDDoS2019 dataset with the goal of examining DDoS assaults using a variety of attack techniques. It is used to analyse attack trends and create effective mitigation tactics, and it is appropriate for testing machine learning-driven intrusion detection systems. Because of its extensive labelling and diversity, the dataset also helps with testing intrusion prevention systems, network traffic behavior, and anomaly detection algorithms.

3.3.1. Real-Time Feedback

According to a number of applications, IoT data can provide insightful feedback in real time, increasing the model's efficacy. It is an essential part of the attack detection system because of this property.

3.3.2. Huge Amount of Data

IoT devices have the capacity to collect vast quantities of data from several sources, guaranteeing precise model performance.

3.3.3. Interconnectivity

IoT devices easily connect the digital and physical worlds, facilitating communication.

Algorithm 1 detects DDoS assaults in 5G networks by utilizing Long Short-Term Memory (LSTM) networks and Harris Hawks Optimization (HHO). Cleaning, standardizing, and dividing traffic into training and testing groups are all part of data preparation. After training the top-performing LSTM model, network traffic is categorized as either DDoS or normal.

Input: DS − Pre-processed 5G traffic dataset

$\delta_{dpr}, \delta_{hdr}, \delta_{lrr}$
−Search ranges for dropout rate, hidden units and learning rate

P_s − Population size, I_{max} −
Maximum number of iterations

Output: Optimized Hyperparameters(μ^*, T^*, α^*)

Evaluation metrics: Accuracy, Precision, Recall, F1, AUC

Step 1: Data Preparation

1.1 Encode categorical features and handle missing values:

$DS \leftarrow \text{Clean}(DS_{raw})$

1.2 Normalize features: $y'_{i,j} = \frac{y_{i,j} - \mu_j}{\sigma_j}, \quad \forall j \in \text{features}$

1.3 Split into training and test sets: $(DS_{train}, DS_{test}) \leftarrow \text{Split}(DS, \lambda)$

Step 2: Harris Hawks Optimization (HHO)

2.1 Initialize hawk population: $P^{(0)} = \{p_i^{(0)} \mid p_i^{(0)} \in \delta_{lrr} \times \delta_{hdr} \times \delta_{dpr}, i = 1, \ldots, N_p\}$

$p_i = (\mu_i, T_i, \alpha_i)$

2.2 Set initial escape energy C_0 and iteration counter $m = 0$

2.3 For $m = 0$ to I_{max}

For each hawk i in population:

Train LSTM with $P_i^{(t)}$ on DS_{train} $k_i^{(t)} = \text{Accuracy}\,(\text{LSTM}(p_i^{(t)}), DS_{val})$

End For

Update positions according to HHO rules:

Exploration phase: $p_i^{(t+1)} = p_r^{(t)} - r_1 \cdot \left| p_r^{(t)} - 2r_2 p_i^{(t)} \right|$

Exploitation phase: $p_i^{(t+1)} = p^* - C \cdot \left| Jp^* - p_i^{(t)} \right|$

Where, $C = 2C_0 \left(1 - \frac{m}{I_{max}}\right)$ - escape energy, J — random jump strength

RESEARCH ARTICLE

$r_1, r_2 \sim U(0,1)$ - random scalars,
p^* - position of best hawk (best fitness so far)

End For

2.4 Select optimal solution: $(\mu^*, T^*, \alpha^*) = \arg \max_{p_i} \alpha_i^{(I_{max})}$

Step 3: Final LSTM Training & Classification

3.1 Train final LSTM:$LSTM^* \leftarrow Train(DS_{train}, \mu^*, T^*, \alpha^*)$

3.2 Predict on test set:$\hat{u} = LSTM^*(DS_{test})$

3.3 Compute evaluation metrics: Accuracy, Precision, Recall, $F_1 - Score$, AUC

Algorithm 1 Using HHO-LSTM to Identify DDoS Attacks in 5G Networks

4. A NEW HHO-BASED METHOD FOR DETECTING DDOS ATTACKS IN NETWORKS USING ADAPTIVE CASCADED LSTM

4.1. HHO Adjusted the Parameter

Inspired by hawk hunting tactics, Heidari and his colleagues created the swarm intelligence-based optimization method known as HHO. Diversification and intensity are two essential elements of the HHO technique, which imitates the actions of predators during a hunt. Exploration is the main emphasis of diversification, but the shift to intensification incorporates strategies like soft, harsh, and mild besiege together with a quick, calculated pounce for efficient optimization.

The paper investigates heuristic algorithm-based DDoS attack detection and mitigation techniques. In order to manage parameters in complicated networks and solve problems with convergence speed, researchers provide novel approaches for accurate parameter tuning. They modify the PCOA method for a range of optimization problems, drawing inspiration from pine cone dynamics. Nevertheless, PCOA's efficacy varies according on the issue, and HHO is a suggested strategy to get around these restrictions.

4.1.1. Diversification

The behavior of HHO is examined in this subsection. In desolate areas, these birds constantly search their surroundings for and discover prey. Harris Hawks use two different hunting methods while perched in random sites. The location of the rabbit and other family members affects their perch position in the first method when d < 0.5 as shown in equation (1).

$$\partial(t+1) = \begin{cases} \partial_{rand}(t) - r_1 \partial''_{rand}(t) - 2r_2 \partial(t), & d \geq 0.5 \\ \partial_{rabbit}(t) - \partial_m(t) - r_3\big(LB + r_4(UB - LB)\big), & d < 0.5 \end{cases} \quad (1)$$

In the second strategy, they use a different hunting method and perch on several tall trees for d ≥ 0.5. Equation (2) determines a parameter's mean value.

$$\partial_m(t) = \frac{1}{N}\sum_{i=1}^{N} \partial_i(t) \quad (2)$$

In the given model, ∂ (t + 1) symbolizes where hawks will be found in the following generation, while ∂rabbit denotes the position of rabbits (prey). The current generation vector is represented by ∂(t). Several random numbers, r1, r2, r3, r4, and d, are generated within the range of 0 to 1 and play a role in the model's calculations. Additionally, r5 is a dynamically chosen hawk, possibly selected based on certain criteria. Another variable, ∂rand, is also involved in the process, though its specific role is not clearly defined. Furthermore, ∂m(t) represents the average position of all hawks as a whole. This formulation appears to be part of a predator-prey simulation or an optimization algorithm, like the HHO algorithm, which Draws inspiration from hawks' cooperative hunting techniques.

4.1.2. Transitioning to Intensification from Diversification

Diversification within the search space is first investigated using optimization techniques, and then the region around the solution is exploited during the intensification phase. The HHO model simulates this process by using the escape energy (C) of the prey, which is represented by a rabbit. If |C| ≥ 1, the diversification process is applied, whereas if |C| < 1, the intensification process takes place. Thus, the transition from diversity to intensification is achieved by using the prey's evaporating energy. The energy estimate is shown below in equation (3).

$$C = C_0\left(1 - \frac{t}{T}\right) \quad (3)$$

4.1.3. Intensification

Four tactics are used in this process: Hard besiege with progressive quick pounce, Soft besiege with progressive quick pounce, hard besiege with progressive quick pounce, and Soft besiege. The next section provides a more thorough explanation of each of these tactics.

- Soft Besiege: In a mild siege, the victim is strong enough to break free but is unable to do so. When |C| ≥ 0.5 and r ≥ 0.5, equation (4) formulates and expresses this situation. The difference between the rabbit's parameter is calculated using equation (5). A scaled random factor is computed using equation (6).

$$\partial(t+1) = \delta\,\partial(t) - C|I \times \partial_{rabbit}(t) - \alpha(t)| \quad (4)$$

$$\delta\,\partial(t) = \partial_{rabbit}(t) - \partial(t) \quad (5)$$

$$I = 2 \times (1 - r_5) \quad (6)$$

RESEARCH ARTICLE

where, r5 is a value between 0 and 1 that is created at random; the jump strength is indicated by I.

- Hard Besiege: The hawk attacks the victim (rabbit) unexpectedly during a heavy besiege since it is unable to flee. When $|C| < 0.5$ and $r \geq 0.5$ equation (7) formulates and states this phenomenon.

$$\partial(t+1) = \partial_{rabbit}(t) - C|\delta\,\partial(t)| \quad (7)$$

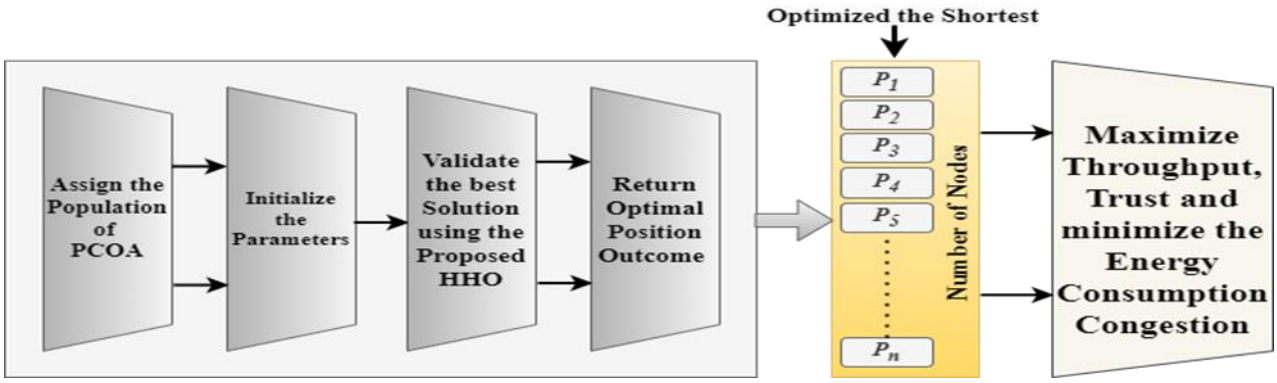


Figure 5 Diagrammatic Illustration of the Optimum Path-Based Attack Mitigation Approach

- Soft Besiege: A gradual swift pounce strategy. The victim might try to flee while still being under a light siege thanks to this tactic. When $|C| < 0.5$ and $r < 0.5$, Compared to the previously mentioned scenario, this one is more adaptable. The L´evy flight function, which models this behavior, is described in equation (8).

$$\partial(t+1) = \begin{cases} R, & \text{if } F(R) < F(\partial(t)) \\ S, & \text{if } F(S) < F(\partial(t)) \end{cases} \quad (8)$$

In this case, R is essential to the hawks' next action and may be expressed as equation (9) and displayed in the following ways.

$$R = \partial_{rabbit}(t) - C|I \times \partial_{rabbit}(t) - \partial(t)| \quad (9)$$

The hawk will occasionally move erratically as it gets closer to its prey. The step size is computed using equation (10). In equation (11) the Lévy flight function is defined. The scaling factor is found using equation (12).

$$S = R + T \times LF(D) \quad (10)$$

$$LF(R) = 0.01 \times \frac{u \times \gamma}{|v|^{\frac{1}{\omega}}} \quad (11)$$

$$\gamma = \left(\frac{\Gamma(1+\omega) \times \sin\left(\frac{\pi\omega}{2}\right)}{\Gamma\left(\frac{1+\omega}{2}\right) \times \omega \times 2^{\frac{\omega-1}{2}}} \right)^{\frac{1}{\omega}} \quad (12)$$

u and v are arbitrary values between 0 and 1, and ω represents a constant value.

- Hard besiege: technique using a gradual rapid pounce. This method relies on the victim's lack of power to flee, and when $|C| < 0.5$ and $r < 0.5$, Over it, a brutal siege is framed. Equation (13), which models and illustrates this behavior. The following is an estimate of the values of R in equation (14) and S equation (15).

$$\partial(t+1) = \begin{cases} R, & \text{if } F(R) < F(\partial(t)) \\ S, & \text{if } F(S) < F(\partial(t)) \end{cases} \quad (13)$$

$$R = \partial_{rabbit}(t) - C|I \times \partial_{rabbit}(t) - \partial(t)| \quad (14)$$

$$S = R + T \times LF(D) \quad (15)$$

4.2. Long Short-Term Memory

In time series forecasting and sequence creation, where knowing the order and connections between data points is essential, LSTM models are frequently utilized. This ability results from the use of gates in the LSTM design that use past data to affect predictions [25] in the future. Depending on how pertinent the knowledge is to the current job, these gates determine whether to keep it or reject it. The external input that is supplied into the cell at time t is represented by the symbol x(t). It often originates from your data sequence, such a sentence's words or sensor readings, and is coupled with the cell's prior hidden state to assist in creating the subsequent hidden state. For tasks like classification or prediction, the model's final output at time t is represented by the symbol y(t). In essence, new information is carried in by x(t), and processed information is carried out of the cell by y(t). During sequential data processing, this technique allows LSTM cells to effectively control and update the information flow across the network. Equation (16) covers the forget gate, Equation (17) covers the input gate, Equation (18) covers the candidate cell state, Equation (19) covers the cell state update, Equation (20) covers the output gate, and Equation (21) covers the final hidden state. These mathematical formulations cover specific operations.

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \quad (16)$$

RESEARCH ARTICLE

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (17)$$

$$\tilde{c_t} = \tanh(W_c[h_{t-1}, x_t] + b_c) \quad (18)$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c_t} \quad (19)$$

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \quad (20)$$

$$h_t = o_t \odot \tanh(c_t) \quad (21)$$

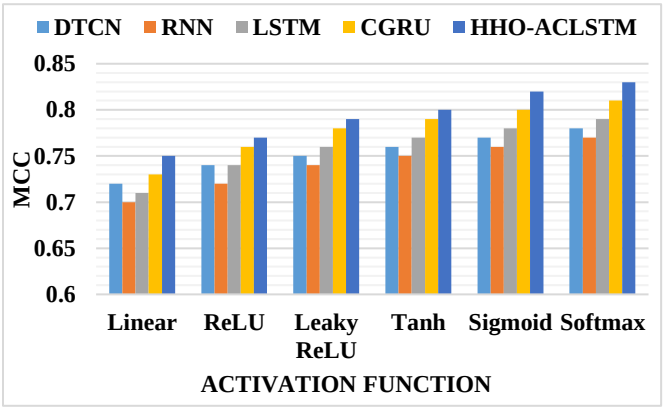
Because LSTMs are skilled at processing and interpreting time-series data, they are excellent at identifying anomalies and treads in network traffic that may point to malicious activity, such as malware, DDoS assaults, or attempts at unauthorized access.

4.3. Adaptive Cascaded LSTM for Detection

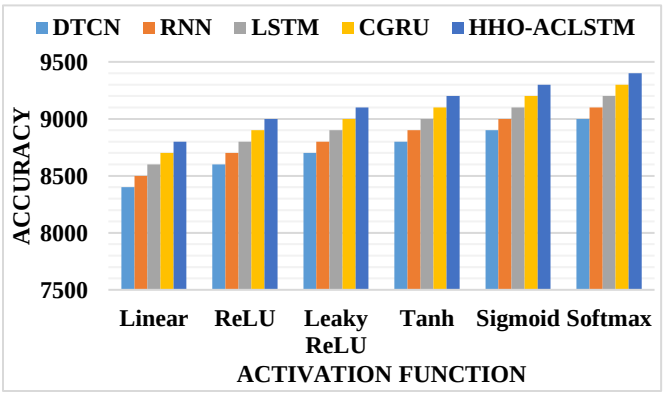
As sophisticated technology advances, DDoS assaults are become more frequent and jeopardizing networks' critical data. like RNN and LSTM have been created and put into use. LSTM Deep learning algorithms that can effectively identify such assaults are therefore required. For this, well-known designs models are very good at capturing long-term relationships, but when trained on big datasets, they can become too generic and prone to overfitting. The training process is further complicated by the fact that LSTMs can have trouble producing new inputs, particularly when processing longer sequences. Furthermore, these deep earning models are made more complex by the difficulties presented by large training data sets and computing limitations. Because of the LSTM model's strong capacity to extract long-term dependencies, we have concentrated on improving it to meet these problems. In contrast to current methods, our improved LSTM model reduces overfitting and delivers higher training efficiency for DDoS attack detection by reducing parameters. However, in some situations, the traditional LSTM still has performance issues. By using a cascaded network design, these issues may be further resolved, which results in the creation of an adaptive cascaded.

LSTM model (ACLSTM), novelty of the Recommended Adaptive Cascaded ACLSTM Framework. They represent the forget gate, input gate, candidate cell state, cell state update, output gate, and final hidden state and offer mathematical formulae for certain procedures. When learning from sequential data, LSTMs perform exceptionally well. More intricate patterns and dependencies over longer sequences may be captured by the model architecture by cascading LSTM layers than could be accomplished by a single LSTM layer. The development of the created Adaptive Cascaded LSTM (ACLSTM) model helps to tackle overfitting concerns, resulting in increased detection performance. To protect critical network data, this model may be trained on sizable and intricate datasets. In order to extract LSTM-based features, the gathered data, or ERa, is fed into the LSTM and goes through a three-step procedure. This iterative process is essential to getting the LSTM's ultimate detection result. This iterative process is essential to getting the LSTM's ultimate detection result. All things considered, this method lowers the FPV, raises the NPV, and improves accuracy. Equation (22) demonstrates the proposed DDoS detection system's goal function.

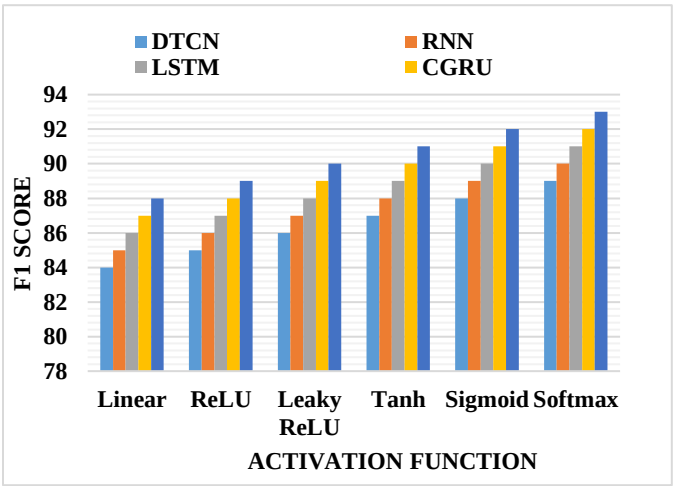
$$\beta_1 = \arg\max(HN_{AG}, EP_{AG}, SP_{AG}) \left(SA + SN + \frac{1}{SF}\right) \quad (22)$$



(a)

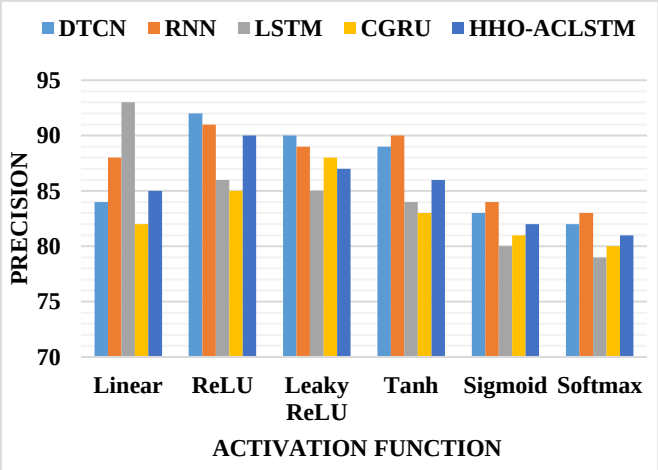


(b)

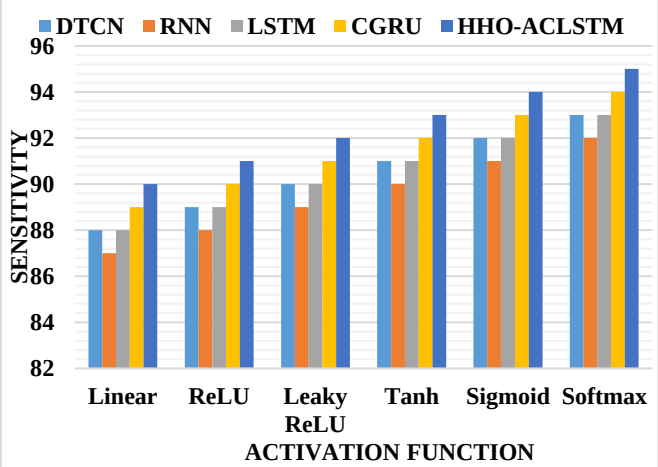


(c)

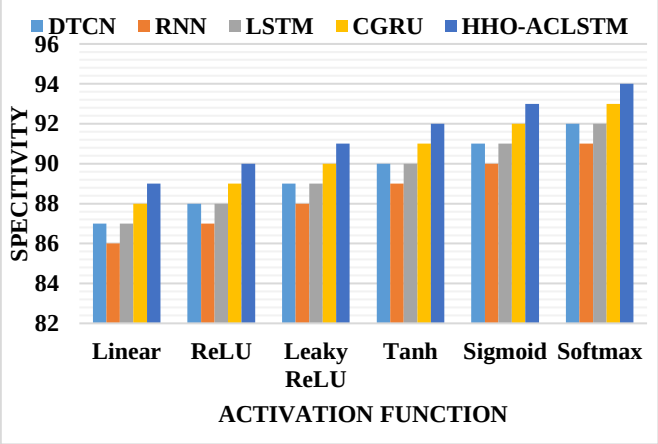
RESEARCH ARTICLE



(d)



(e)



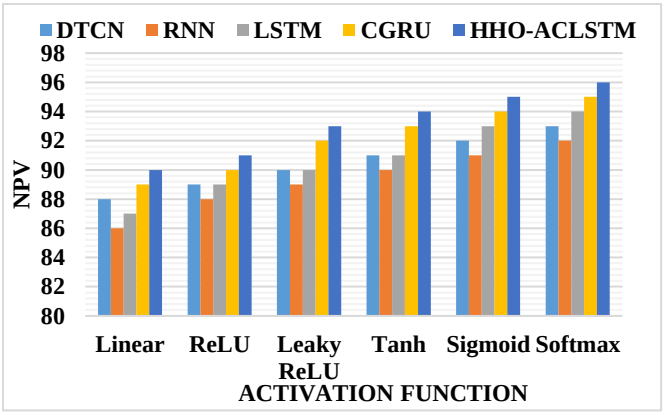
(f)

Figure 6 Analysis of the Designed HHO-Based DDoS Attack Detection Activation Function in 5G Networks (a) MCC (b)Accuracy (c) F 1 Score (d) Precision (e) Sensitivity (f) Specitivity

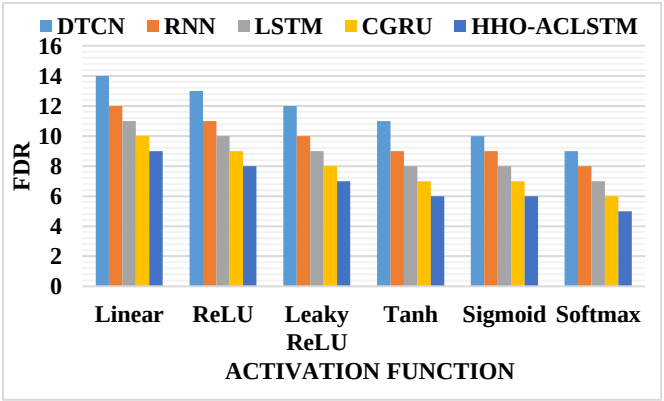
Here, the variables HNAG, EPAG, and SPAG denote the hidden neuron count, epoch count, and steps per epoch in the ACLSTM model, respectively. The values for these parameters range over predefined intervals. Furthermore, SA, SN, and SF make reference to the FNR, NPV, and accuracy, accordingly. Figure. 4 displays the suggested perspective of the proposed ACLSTM detection model.

4.4. An Architectural Illustration of the ACLSTM Model that was Developed

The created ACLSTM concept is used to mitigate the DDoS assault. This framework extracts LSTM-based features for assessing model performance by first feeding the gathered input data into an LSTM layer and then repeating the procedure three times. The several gates that comprise the LSTM network are the forget gate, input gate, candidate cell state, and output gate. This gating mechanism facilitates the efficient flow of information throughout the network and enables high detection accuracy in recognizing DDoS attacks. To efficiently handle complicated input and generate trustworthy results, the network's hidden state is updated at every time step. Finally, to differentiate between data that has been attacked and data that has not, the ACLSTM model generates a binary output (0 or 1).



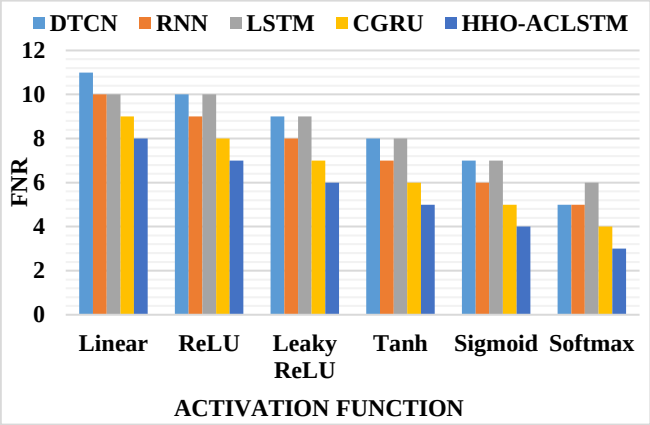
(a)



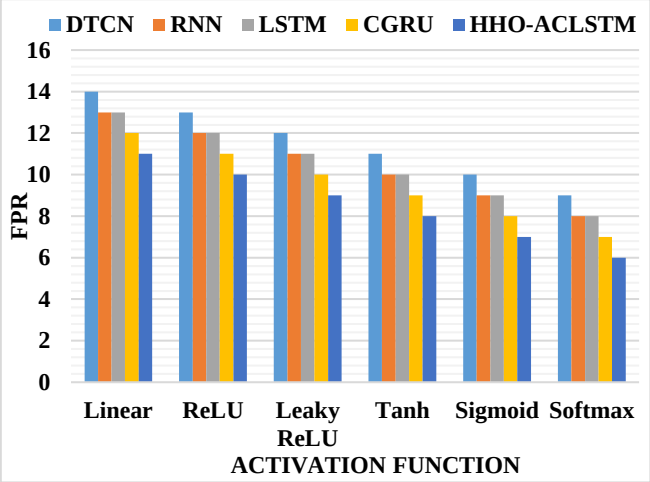
(b)

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/38 Volume 12, Issue 4, July – August (2025)

RESEARCH ARTICLE



(c)



(d)

Figure 7 Analysis of the Designed HHO-Based DDoS Attack Detection Activation Function in 5G Networks (a) NPV or Negative Predictive Value b) Rates of False Discovery (FDR) (c) False Negative Rate (FNR) (d) False Positive Rate (FPR)

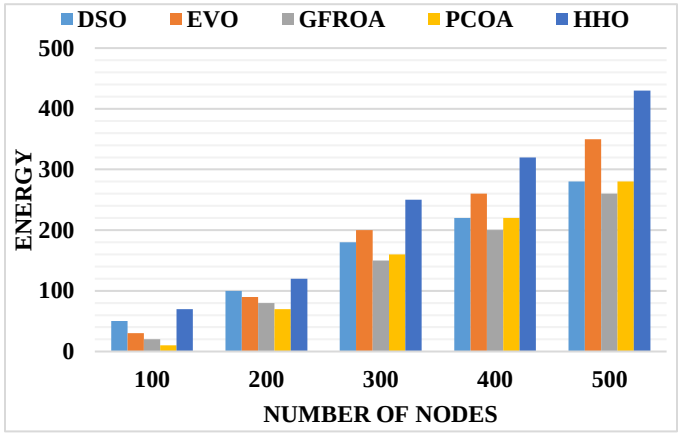
5. USE OPTIMUM ROUTING WITH ITS GOAL FUNCTION AND LIMITATIONS TO LESSEN ASSAULTS

5.1. Using the Best Way to Mitigate Attacks

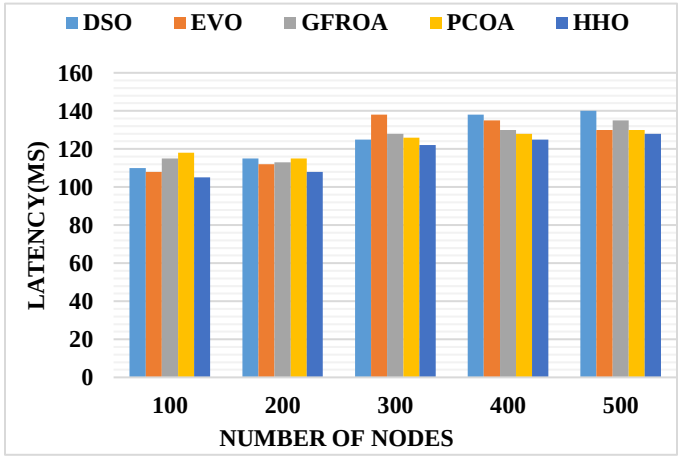
Using optimum pathways for attack mitigation is a crucial tactic in the field of network security[31], especially in contemporary 5G networks, to fend off malevolent actions like DDoS attacks [32]. By focusing on finding and using the most effective data transmission channels, this strategy improves the overall resilience of the network while maintaining the availability and integrity of network services. The technique reduces the effect of assaults by carefully controlling data flow along these ideal channels, guaranteeing the security and continuity of vital network operations and services.

Network route optimization turns become a crucial proactive cybersecurity tool, especially for protecting the cutting-edge 5G network infrastructures, which are rapidly becoming the backbone of modern digital communication and the Internet of Things. Figure 5 illustrates the concept of attack mitigation using an optimal strategy. Anticipated advantages for data transmission and network security: The technology guarantees strong network security and promotes better data transfer between the nodes by examining the attack detection and mitigation approach. This assessment precisely guards against extensive network assaults and reduces network outages. The shortest path is found when the created HHO algorithm finds an ideal solution.

This ensures higher-quality data transfer and successfully identifies attack patterns in both benign and malevolent network traffic. This method improves overall system performance on a strong network architecture by managing more datasets and minimizing needless mitigation measures. Data transfer and network security are greatly improved by this performance boost.



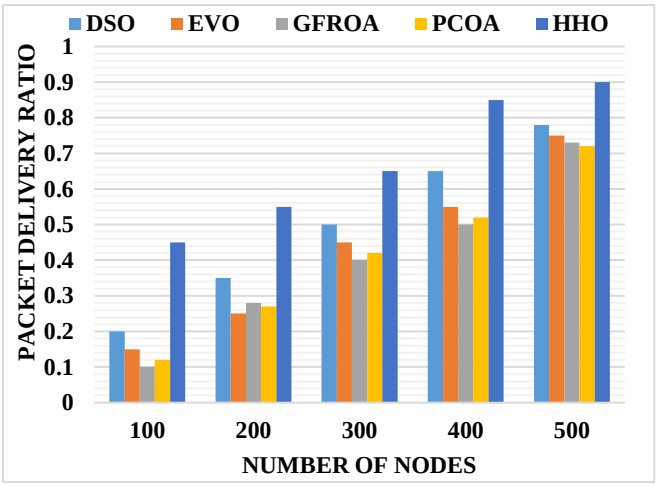
(a)



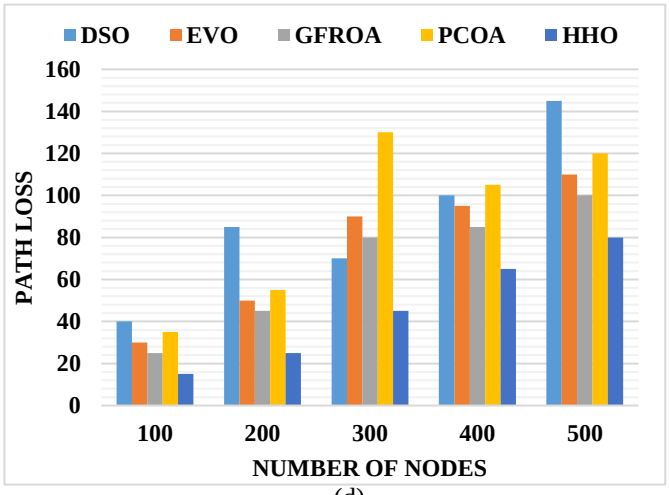
(b)

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/38 Volume 12, Issue 4, July – August (2025)

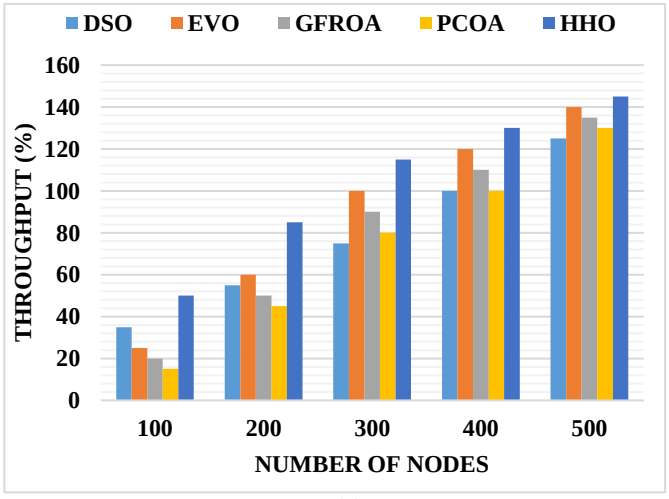
RESEARCH ARTICLE



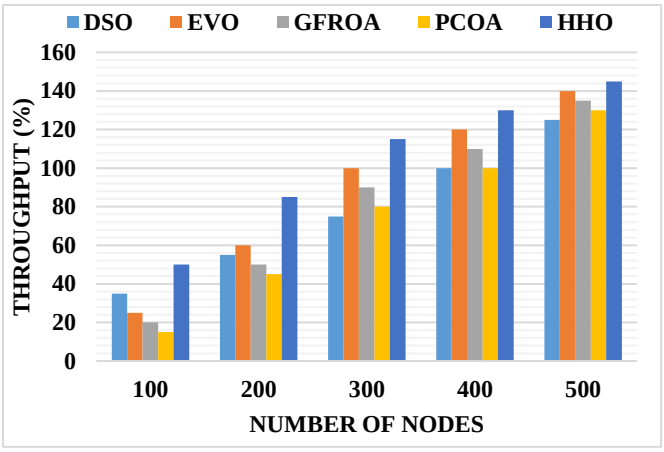
(c)



(d)



(e)



(f)

Figure 8 Using Conventional Algorithms for Optimal Routing in the Mitigation Model with Regard to:(a) Energy (b) Latency (c) Packet Delivery Ratio(PDR) (d) Path Loss (e) Throughput (f) Trust

5.2. Objective Function

The goal of an optimal path strategy is to prevent or lessen the effects of DDoS assaults by determining and putting into practice the best path for data to take when moving across a network. This step uses the observed data as its input. Data packets may travel longer paths to get to their destination if the quickest or most efficient path is not optimized, which greatly raises latency and impairs the performance of real time applications.

The suggested HHO method is applied to address these problems by utilizing optimization techniques that concentrate on factors like the shortest path. In order to improve performance, this procedure mainly adjusts the model parameters, which lowers energy consumption and increases network trust and throughput. The suggested DDoS mitigation system's objective function is shown in in equation (23).

$$\beta_2 = arg \max_{\{p_n\}} \left(Tr + Th + \frac{1}{EC} \right) \quad (23)$$

The variable pn indicates the ideal number of nodes for the shortest path, which is shown as p1, p2, . . ., p_n. The terms T r, T h, and EC refer to trust, throughput, and energy consumption, respectively.

5.3. Performance Indicators for the Suggested DDoS Defense System

The following restrictions apply to the multi-objective function once the DDoS assault has been mitigated.

- Trust: The way that direct and indirect trust are included into a core framework is frequently arbitrary and can change based on the situation. This idea is analytically

RESEARCH ARTICLE

stated in equation (24), where indirect trust is obtained from third-party suggestions or experiences, while direct trust is defined as the trust that results from direct contacts between entities.

$$Tr = \alpha U_{dir} + (1 - \alpha)U_{indir} \quad (24)$$

Here, the terms U_{indir} and U_{dir} denote indirect, direct trust, respectively.

- Throughput: It may be expressed as the total quantity of data that is successfully transmitted over a network in a specific length of time using equation (25).

$$Th = \frac{\sum_{i=1}^{v} K_y}{s} \quad (25)$$

In this context, Ky symbolizes the total number of packets received, v indicates how many packets there are, and s represents the time frame.

- Energy consumption: The overall energy usage of all transmitting and receiving nodes are determined by equation (26).

$$EC = \sum_{i=1}^{v}\{(W_{ty,i} + W_{iy,i})\} \quad (26)$$

The terms $W_{ty,i}$ and $W_{iy,i}$ reflect a node's power consumption while transmitting and receiving, respectively.

Table 2 The Suggested Deep Learning-Based DDoS Attack Detection and Mitigation Approach for 5G Networks Includes a Statistical Analysis of Conventional Techniques

TERMS	DSO [26]	EVO [27]	GFROA [28]	PCOA[29]	EEPCO[30]	HHO
Number of nodes: 100						
Mean	0.000295	0.000298	0.000399	0.000338	0.000276	0.000267
Best	0.000292	0.000291	0.000384	0.000323	0.00027	0.000210
Worst	0.000318	0.000409	0.000450	0.000420	0.000355	0.000320
Median	0.000292	0.000291	0.000384	0.000323	0.000270	0.000121
Standard deviation	7.12×10^{-6}	2.43×10^{-5}	2.57×10^{-5}	2.04×10^{-5}	1.57×10^{-5}	1.37×10^{-5}
Number of nodes: 200						
Median	0.000318	0.00032	0.000455	0.000348	0.000295	0.000231
Worst	0.000344	0.000481	0.000521	0.000455	0.000381	0.000256
Mean	0.000322	0.00033	0.00047	0.000364	0.000302	0.000209
Standard deviation	8.09×10^{-6}	3.42×10^{-5}	2.57×10^{-5}	2.12×10^{-5}	1.65×10^{-5}	1.45×10^{-5}
Best	0.000318	0.00032	0.000455	0.000348	0.000295	0.000245
Number of nodes: 300						
Standard deviation	9.93×10^{-6}	3.15×10^{-5}	1.83×10^{-5}	1.79×10^{-5}	1.53×10^{-5}	1.33×10^{-5}
Worst	0.000363	0.000486	0.000524	0.000449	0.000402	0.000340
Median	0.000332	0.000339	0.000475	0.000355	0.000314	0.000241
Best	0.000332	0.000339	0.000475	0.000355	0.000314	0.000234
Mean	0.000337	0.000349	0.000485	0.000366	0.000320	0.000310
Number of nodes: 400						
Standard deviation	2.46×10^{-5}	2.49×10^{-5}	2.07×10^{-5}	1.83×10^{-5}	1.50×10^{-5}	1.20×10^{-5}
Worst	0.000474	0.000366	0.000459	0.000499	0.000454	0.000367
Mean	0.000363	0.000341	0.000348	0.000456	0.000375	0.000265

RESEARCH ARTICLE

Best	0.000356	0.000337	0.00034	0.000444	0.000362	0.000319
Median	0.000356	0.000337	0.00034	0.000444	0.000362	0.000245
Number of nodes: 500						
Worst	0.000382	0.000474	0.000515	0.000477	0.000420	0.000239
Median	0.000354	0.000356	0.000454	0.000383	0.000334	0.000289
Standard deviation	7.84×10^{-6}	2.46×10^{-5}	2.32×10^{-5}	1.93×10^{-5}	1.54×10^{-5}	1.14×10^{-5}
Best	0.000354	0.000356	0.000454	0.000383	0.000334	0.000233
Mean	0.000358	0.000363	0.000468	0.000396	0.000340	0.000245

Table 3 For 5G Networks, the Suggested Deep Learning-Based DDoS Attack Detection and Mitigation Model Outperforms Conventional Classifiers and Algorithm

Algorithm Comparison						
TERMS	DSO-ACGRU [33]	EVO-ACGRU [34]	GFROA-ACGRU [35]	PCOA-ACGRU [36]	EEPCO-ACGRU [37]	HHO-ACLSTM
MCC	83.10	82.90	83.90	85.04	88.10	89.05
F1-Score	91.76	91.57	92.12	92.52	94.18	95.03
FDR	08.99	08.20	08.28	06.17	06.32	06.12
NPV	90.54	91.56	91.35	93.80	93.39	93.98
FNR	07.47	08.65	07.47	08.75	05.31	05.04
FPR	09.46	08.44	08.65	06.21	06.61	06.05
Precision	91.01	91.80	91.72	93.83	93.68	93.89
Specificity	90.54	91.56	91.35	93.80	93.39	93.45
Sensitivity	92.53	91.35	92.53	91.25	94.69	94.87
Accuracy	91.55	91.45	91.95	92.51	94.05	94.95
Classifier Comparison						
TERMS	DTCN[24]	LSTM [25]	RNN [32]	CGRU [33]	EEPCO-ACGRU[34]	HHO-ACLSTM
MCC	80.71	81.00	84.10	84.90	88.10	89.43
F1-Score	90.63	90.71	92.25	92.60	94.18	95.20
FDR	10.46	09.82	08.51	07.71	06.32	05.96
NPV	88.91	89.73	91.05	91.96	93.39	94.78
FNR	08.26	08.75	06.98	07.08	05.31	05.23
FPR	11.09	10.28	08.95	08.04	06.61	05.34
Precision	89.54	90.19	91.49	92.29	93.68	94.56
Specificity	88.91	89.73	91.05	91.96	93.39	94.23
Sensitivity	91.74	91.25	93.02	92.92	94.69	94.99
Accuracy	90.35	90.50	92.05	92.45	94.05	95.03

RESEARCH ARTICLE

6. RESULTS AND ANALYSIS FROM SIMULATIONS

A number of steps are taken in order to verify the outcomes prior to system deployment. In 5G-enabled IoT networks, DDoS assaults are effectively detected and mitigated using the Python platform. Improved performance is guaranteed by the network's architecture, which improves attack detection and mitigation procedures. Comparisons with current techniques show how successful the recently created detection and mitigation system. Each of the 100 cycles that make up the initialization process the population evenly dispersed.

Table 4 Our Research Presents a New DDoS Attack Prevention Method for 5G IoT Networks

TERMS	AE-BGRU [34]	ADA [35]	CC-LSTM [38]	EDBN [39]	EEPCO-ACGRU [40]	HHO-ACLSTM
MCC	75.32	75.63	78.22	77.90	88.10	89.23
Accuracy	87.65	87.08	89.01	88.95	94.05	95.43
F1-Score	88.05	88.21	89.44	89.25	94.18	95.20
Precision	86.67	86.71	88.16	88.34	93.68	94.03
Sensitivity	89.48	89.77	90.76	90.17	94.69	95.02
Specificity	85.76	85.76	87.39	87.69	93.39	94.06
NPV	85.76	85.74	87.78	87.37	93.50	94.45
FDR	13.33	13.30	11.84	11.66	06.32	06.12
FNR	10.52	10.23	09.24	09.83	05.31	05.01
FPR	14.24	14.24	12.61	12.31	06.61	06.03

The model's overall performance is enhanced by the structured initialization step, which produces more successful optimization outcomes. By comparing the proposed model with other techniques, including the Drone Squadron Optimization, Energy Valley Optimizer, and Grass Fibrous Root Optimization Algorithm, its efficacy is evaluated [33]. Furthermore, it is compared to classifiers like DTCN, RNN, LSTM, and CGRU. Also taken into consideration for comparison are modern state-of-the-art methods such as AdaBoost [34], CC-LSTM, Enhanced DBN, and Autoencoder with a Bidirectional Gated Recurrent Unit [35]. The model's performance indicators were successfully evaluated to guarantee accuracy, indicating its efficacy in enhancing detection and mitigation results

- Recall: The accurate values are determined by t. It can be seen in equation (27).

$$\text{Recall} = \frac{m}{m+q} \quad (27)$$

- Specificities: Equation (28) provides a suitable expression for the negative results.

$$\text{Specificity} = \frac{n}{n+p} \quad (28)$$

- Precision: Describes the proportion of precise and correct examples from the provided data and is also stated in equation (29).

$$\text{Precision} = \frac{m}{m+p} \quad (29)$$

- Proportion of False Positives (FPR): Negative data examples are represented by equation (30), which facilitates categorization. These examples distinguish between actual and non-occurrences and are not part of the target class. By increasing detection accuracy, analyzing negative cases boosts the model's dependability and effectiveness.

$$\text{FPR} = \frac{p}{p+n} \quad (30)$$

- False Negative Rate: Test results are negative for the positive instances in the data. It may be found in equation (31).

$$\text{FNR} = \frac{q}{q+m} \quad (31)$$

- Negative Predictive Value (NPV): True negative numbers are taken into account for test outcomes. Equation (32) provides an illustration of it.

$$\text{NPR} = \frac{b}{b+d} \quad (32)$$

- False Discovery Rate (FDR): The FDR shows the number of rejections from false positives as well as the number of true positives. Equation (33) provides a representation of it.

$$\text{FDR} = \frac{p}{p+m} \quad (33)$$

- F1-Score: In equation (34), the F1-score is confirmed.

RESEARCH ARTICLE

$$\text{F1} - \text{Score} = \frac{2*\text{precision}*\text{recall}}{\text{precision}+\text{recall}} \quad (34)$$

- Matthews Statistical Measure (MCC): The quality during the testing phase is depicted in equation (35).

$$\text{MCC} = \frac{\text{m}*\text{n}-\text{p}*\text{q}}{\sqrt{(\text{m}+\text{p})(\text{m}+\text{n})(\text{n}+\text{p})(\text{n}+\text{q})}} \quad (35)$$

95.02% sensitivity, and 94.45% accuracy. The Harris Hawk Optimization (HHO) integration of the system enhances generalization across traffic circumstances and lowers false alarm rates. The framework's high dependability and good discriminating abilities are confirmed by its AUC-ROC score of 0.961. Additionally, the results are better due to the combination of Harris Hawk Optimization for parameter tuning and Adaptive Cascaded LSTM for modelling temporal patterns. This combination ensures safe and effective data transmission routing while enhancing detection and reducing false rates.

Table 5 A Comparison of the Most Advanced, Contemporary Optimization Techniques with the Created HHO

TERMS	IGOA [39]	ASS-JSLNO [40]	HBO [41]	EEPCO [42]	Proposed HHO
MCC	76.81	78.89	77.92	88.10	89.65
Accuracy	88.40	89.45	88.95	94.05	95.63
F1-Score	88.75	89.67	89.29	94.18	95.98
Precision	87.56	89.28	88.05	93.68	94.45
Sensitivity	89.97	90.07	90.56	94.69	95.02
Specificity	86.78	88.81	87.28	93.39	94.56
NPV	86.78	88.81	87.28	93.39	94.35
FDR	12.44	10.72	11.95	06.32	05.67
FNR	10.03	09.93	09.44	05.31	04.98
FPR	13.23	11.19	12.72	06.61	05.89

Table 6 Recent Studies Evaluated the Performance of the Suggested Model with Current Approaches in Terms of Specificity, F1-Score, Recall, Precision and Accuracy

S. No.	Model	Author	Year	AUC	F1-Score	Recall	Precision	Accuracy
1	AE-BGRU	Aljebreen et al. [11]	2023	84.95	85.72	86.10	85.34	87.65
2	EDBN	Tseng et al., [25]	2023	85.80	87.52	87.85	87.20	88.95
3	GOA-LSTM	Wahab et al., [29]	2024	86.75	88.80	89.00	88.60	89.05
4	CGRU	Akhtar et al.,[31]	2025	88.60	89.90	90.00	89.80	90.20
5	DTCN	Sadhwani et al. [42]	2025	91.30	90.60	90.90	90.75	89.89
6	Proposed Model	Ji et al.	2025	94.56	95.10	95.02	95.20	94.45

RESEARCH ARTICLE

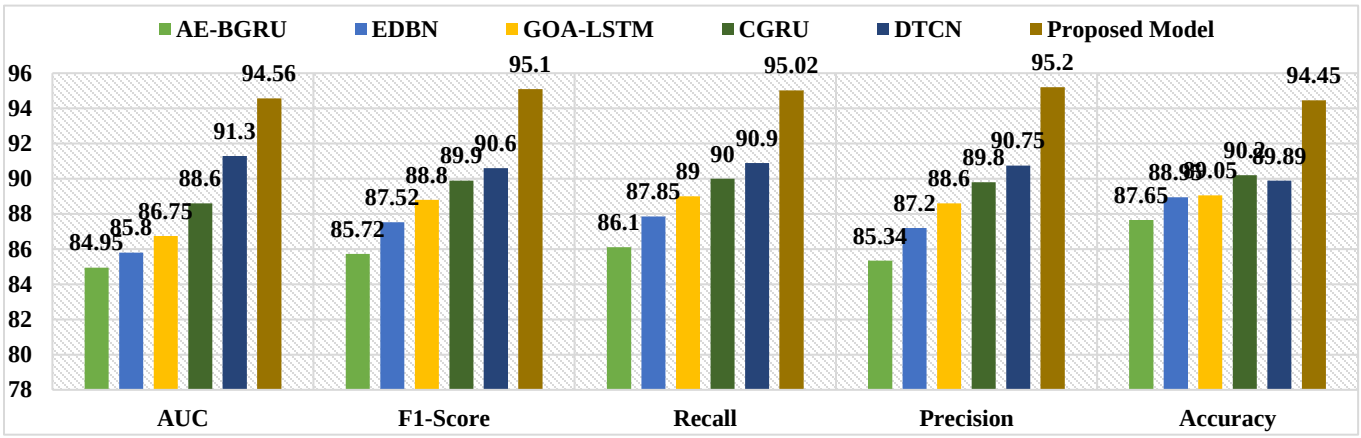


Figure 9 Performance Comparison of Various Models Based on Specificity, F1-Score, Recall, Precision, and Accuracy

6.1. Performance Measurements' Importance

Performance indicators such as accuracy, precision, recall, F1-score, specificity, False Negative Rate, False Discovery Rate, and False Positive Rate are used to assess the quality and consistency of the suggested DDoS attack detection model. Reduced misclassifications and better classification outcomes are achieved using smaller error-based measurements. In real-time 5G networks, the model exhibits better detection accuracy, error reduction, and decision making robustness when compared to other detection models.

7. CONCLUSION

Our study offers a novel defense strategy against DDoS assaults in 5G IoT networks. In order to identify and mitigate attacks in 5G settings, we have presented the sophisticated ACLSTM model with the ground-breaking HHO algorithm. The dependability and availability of 5G networks depend on this deep learning-based method's capacity to identify DDoS assaults with high accuracy and few false positives. It significantly strengthens 5G IoT networks' resistance to DDoS assaults by improving the ACLSTM model's variables to identify the most effective data transmission channel. Network security is greatly improved by the present deep learning model because of its effectiveness and versatility. Comparative findings show that the accuracy of 94.05% is superior to that of AE-BGRU 87.65%, ADA 87.8%, CC-LSTM 89.01%, and EDBN 88.95%. Additionally, the suggested detection model shows significant gains over DTCN up 23.09%, GOA-LSTM up 89.05%, RNN 11.2%, and CGRU up 90.2%. These results demonstrate how much more successful the model is than traditional classifier models. However, it is still difficult to strike the ideal balance between reducing false positives and negatives. Even little errors might lead to missed dangers or service interruptions in dynamic contexts. For a stronger protection against multi-vector assaults, future research should combine DDoS detection with other network security layers. Techniques for feature selection, data balance, and preprocessing step evaluation will be investigated. We'll take into account validation in various IoT contexts and real-world situations. Preventive steps and the difficulties brought on by different network configurations and advanced attack techniques will be examined. Federated learning for distributed detection, explainable AI tools for transparency and trust, and the integration of Zero Trust security architectures and blockchain-based access control can all enhance the suggested paradigm. Its scalability and resilience are confirmed by real-time deployment in 5G use cases such as autonomous cars and smart healthcare.

REFERENCES

[1] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama, and M. A. Hamza, "Enhancing DDoS attack detection using snake optimizer with ensemble learning on internet of things environment," IEEE Access, vol. 11, pp. 104745–104753, 2023.

[2] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. Ben Dhaou, "Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model," IEEE Access, vol. 11, pp. 119862–119875, 2023.

[3] Z. Liu, C. Guo, D. Liu, and X. Yin, "An asynchronous federated learning arbitration model for low-rate ddos attack detection," IEEe Access, vol. 11, pp. 18448–18460, 2023.

[4] H. Huang, P. Ye, M. Hu, and J. Wu, "A multi-point collaborative DDoS defense mechanism for IIoT environment," Digit. Commun. Networks, vol. 9, no. 2, pp. 590–601, 2023.

[5] N. Sivanesan and K. S. Archana, "RETRACTED ARTICLE: Detecting distributed denial of service (DDoS) in SD-IoT environment with enhanced firefly algorithm and convolution neural network," Opt. Quantum Electron., vol. 55, no. 5, p. 393, 2023.

[6] A. Alashhab, M. S. Zahid, A. Muneer, and M. Abdullahi, "Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks," Authorea Prepr., 2022.

[7] S. Yousef Alshunaifi, S. Mishra, and M. Alshehri, "Cyber-Attack Detection and Mitigation Using SVM for 5G Network.," Intell. Autom. \& Soft Comput., vol. 31, no. 1, 2022.

[8] R. M. Alzhrani and M. A. Alliheedi, "5g networks and iot devices: Mitigating ddos attacks with deep learning techniques," arXiv Prepr. arXiv2311.06938, 2023.

[9] M. A. HUSSAIN, A. U. BEGUM, Z. SYED, and D. R. M. S. AL ANSARI, "Dynamic slicing optimization in 5G networks using a recursive LSTM mechanism with grey wolf optimization," J. Theor. Appl. Inf. Technol., vol. 102, no. 2, pp. 569–583, 2024.

[10] M. Alauthman, A. Aldweesh, A. Al-Qerem, A. Y. Al Maqousi, A.

RESEARCH ARTICLE

Almomani, and M. Alkasassbeh, "Cryptographic protocols for internet of things (IoT) security lightweight schemes and practical deployment," Innov. Mod. Cryptogr., pp. 431–448, 2024.
[11] P. Benlloch-Caballero, Q. Wang, and J. M. A. Calero, "Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks," Comput. Networks, vol. 222, p. 109526, 2023.
[12] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks," Ieee Access, vol. 11, pp. 28934–28954, 2023.
[13] R. Jmal, W. Ghabri, R. Guesmi, B. M. Alshammari, A. S. Alshammari, and H. Alsaif, "Distributed blockchain-SDN secure IoT system based on ANN to mitigate DDoS attacks," Appl. Sci., vol. 13, no. 8, p. 4953, 2023.
[14] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "A DDoS attack mitigation framework for IoT networks using fog computing," Procedia Comput. Sci., vol. 182, pp. 13–20, 2021.
[15] I. A. Khan, M. Keshk, D. Pi, N. Khan, Y. Hussain, and H. Soliman, "Enhancing IIoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems," Ad Hoc Networks, vol. 134, p. 102930, 2022.
[16] I. A. Khan, D. Pi, M. Z. Abbas, U. Zia, Y. Hussain, and H. Soliman, "Federated-SRUs: A federated-simple-recurrent-units-based IDS for accurate detection of cyber attacks against IoT-augmented industrial control systems," IEEE Internet Things J., vol. 10, no. 10, pp. 8467–8476, 2022.
[17] A. Singh and B. B. Gupta, "Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," Int. J. Semant. Web Inf. Syst., vol. 18, no. 1, pp. 1–43, 2022.
[18] A. Mishra, B. K. Joshi, V. Arya, A. K. Gupta, and K. T. Chui, "Detection of distributed denial of service (DDoS) attacks using computational intelligence and majority vote-based ensemble approach," Int. J. Softw. Sci. Comput. Intell., vol. 14, no. 1, pp. 1–10, 2022.
[19] E. M. Bårli, A. Yazidi, E. H. Viedma, and H. Haugerud, "DoS and DDoS mitigation using variational autoencoders," Comput. Networks, vol. 199, p. 108399, 2021.
[20] A. Mishra, N. Gupta, and B. B. Gupta, "Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller," Telecommun. Syst., vol. 77, no. 1, pp. 47–62, 2021.
[21] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks," IEEE Trans. Ind. Informatics, vol. 18, no. 11, pp. 8356–8366, 2022.
[22] D. Namakshenas, A. Yazdinejad, A. Dehghantanha, and G. Srivastava, "Federated quantum-based privacy-preserving threat detection model for consumer internet of things," IEEE Trans. Consum. Electron., vol. 70, no. 3, pp. 5829–5838, 2024.
[23] A. Yazdinejad, A. Dehghantanha, G. Srivastava, H. Karimipour, and R. M. Parizi, "Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Things," J. Syst. Archit., vol. 148, p. 103088, 2024.
[24] M. D. M. Akhtar, R. S. A. Shatat, A. S. A. Shatat, S. A. Hameed, and S. Ibrahim Alnajdawi, "IoMT-based smart healthcare monitoring system using adaptive wavelet entropy deep feature fusion and improved RNN," Multimed. Tools Appl., vol. 82, no. 11, pp. 17353–17390, 2023.
[25] M. M. Akhtar, S. A. Alasmari, S. W. Haidar, and A. A. Alzubaidi, "Distributed denial of service attack detection and mitigation strategy in 5G-enabled internet of things networks with adaptive cascaded gated recurrent unit," Peer-to-Peer Netw. Appl., vol. 18, no. 2, p. 81, 2025.
[26] M. R. Rao and S. Sundar, "An efficient method for optimal allocation of resources in LPWAN using hybrid coati-energy valley optimization algorithm based on reinforcement learning," IEEE Access, vol. 11, pp. 116169–116182, 2023.
[27] H. Shi, J. Li, and N. Zafetti, "RETRACTED: New optimized technique for unknown parameters selection of SOFC using Converged Grass Fibrous Root Optimization Algorithm," 2020, Elsevier.
[28] M. Valikhan Anaraki and S. Farzin, "The pine cone optimization algorithm (PCOA)," Biomimetics, vol. 9, no. 2, p. 91, 2024.
[29] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," IEEE access, vol. 9, pp. 161546–161554, 2021.
[30] Z. Khan, M. Chowdhury, M. Islam, C.-Y. Huang, and M. Rahman, "Long short-term memory neural network-based attack detection model for in-vehicle network security," IEEE Sensors Lett., vol. 4, no. 6, pp. 1–4, 2020.
[31] M. Dabbaghjamanesh, A. Moeini, J. Kimball, and J. Zhang, "Using gated recurrent units for selective harmonic current mitigation-pwm in grid-tied cascaded h-bridge converters," IEEE Trans. Ind. Appl., 2020.
[32] A. Mezina, R. Burget, and C. M. Travieso-González, "Network anomaly detection with temporal convolutional network and U-Net model," IEEE Access, vol. 9, pp. 143608–143622, 2021.
[33] H. Singh, S. Sharma, M. Khurana, M. Kaur, and H.-N. Lee, "Binary Drone Squadron optimization approaches for feature selection," IEEE Access, vol. 10, pp. 87099–87114, 2022.
[34] W. G. Gadallah, H. M. Ibrahim, and N. M. Omar, "A deep learning technique to detect distributed denial of service attacks in software-defined networks," Comput. \& Secur., vol. 137, p. 103588, 2024.
[35] K. K. Paidipati, C. Kurangi, J. Uthayakumar, S. Padmanayaki, D. Pradeepa, and S. Nithinsha, "Ensemble of deep reinforcement learning with optimization model for DDoS attack detection and classification in cloud based software defined networks," Multimed. Tools Appl., vol. 83, no. 11, pp. 32367–32385, 2024.
[36] Y. A. Abid, J. Wu, G. Xu, S. Fu, and M. Waqas, "Multilevel deep neural network approach for enhanced distributed denial-of-service attack detection and classification in software-defined Internet of Things networks," IEEE Internet Things J., vol. 11, no. 14, pp. 24715–24725, 2024.
[37] D. Durairaj, T. K. Venkatasamy, A. Mehbodniya, S. Umar, and T. Alam, "Intrusion detection and mitigation of attacks in microgrid using enhanced deep belief network," Energy Sources, Part A Recover. Util. Environ. Eff., vol. 46, no. 1, pp. 1519–1541, 2024.
[38] V. R. S. Dora and V. N. Lakshmi, "Smart network security using advanced ensemble-DDoS attack detection and hybrid JA-SLOA-linked optimal routing-based mitigation," Aust. J. Electr. Electron. Eng., vol. 21, no. 4, pp. 374–396, 2024.
[39] O. Pandithurai, C. Venkataiah, S. Tiwari, and N. Ramanjaneyulu, "DDoS attack prediction using a honey badger optimization algorithm based feature selection and Bi-LSTM in cloud environment," Expert Syst. Appl., vol. 241, p. 122544, 2024.
[40] C. H. Tseng and Y.-T. Chang, "EBDM: Ensemble binary detection models for multi-class wireless intrusion detection based on deep neural network," Comput. \& Secur., vol. 133, p. 103419, 2023.
[41] F. Wahab, A. Shah, I. Khan, B. Ali, and M. Adnan, "An SDN-based Hybrid-DL-driven cognitive intrusion detection system for IoT ecosystem," Comput. Electr. Eng., vol. 119, p. 109545, 2024.
[42] S. Sadhwani, A. Mathur, R. Muthalagu, and P. M. Pawar, "5G-SIID: an intelligent hybrid DDoS intrusion detector for 5G IoT networks," Int. J. Mach. Learn. Cybern., vol. 16, no. 2, pp. 1243–1263, 2025.

Authors

Sharma Ji has been pursuing a Ph.D. in Computer Science and Engineering at IFTM University in Moradabad since 2022. He has been helping to conduct undergraduate and graduate courses at Ajay Kumar Garg Engineering College Ghaziabad as an Assistant Professor in the Department of Computer Science and Engineering. His primary areas of interest in research include computer networking, machine learning, and cryptography, with a focus

RESEARCH ARTICLE

on network security and the creation of clever methods for identifying risks in the emerging domains of 5G and the Internet of Things. In well-known international journals and conferences, he has co-discovered and co-authored a few research pieces.

Dr. Abhishek Mishra working as a Professor in Department of Computer Science & Engineering, School of Computing Science & Applications in IFTM University, Moradabad, U.P. He completed MCA and M.Tech from RGPV Bhopal. He has been nearly two decades of experience in teaching and his areas of specializations are Machine Learning, Artificial Intelligence, Image Processing, Network security. He has published 8 patents and 35+ papers in international journals/ Conference proceedings. Dr. Mishra also supervised one candidate as PhD research scholar and published three books on machine learning. He has participated in several National Workshop, International Conferences and Technical Events. He is regularly invited to deliver lectures in various programmers for imparting skills in research methodology to students and research scholars.

How to cite this article:

Sharma Ji, Abhishek Mishra, "Enhancing DDoS Detection and Mitigation in 5G Networks Using LSTM and Harris Hawk Optimization", International Journal of Computer Networks and Applications (IJCNA), 12(4), PP: 631-651, 2025, DOI: 10.22247/ijcna/2025/38.