Electrical Engineering Technical Journal, ISSN: 3007-9772, Vol. 2, No. 2, 2025, Pages 25-32
DOI: https://doi.org/10.51173/eetj.v2i2.25

Electrical Engineering Technical Journal
Journal homepage: http://eetj.mtu.edu.iq

RESEARCH ARTICLE

NS-3-Based Modeling and Detection of DDoS Attacks in Internet of Things Networks

Ali S. Kurji [1*]

[1] Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq

* Corresponding Author Email: ali.alrubaie@mtu.edu.iq

Article Info.

Article history:

Received
11 May 2025

Accepted
29 June 2025

Published in Journal
30 June 2025

Abstract

The Internet of Things has expanded rapidly in recent years, introducing new capabilities into everyday devices while simultaneously exposing those systems to increasingly sophisticated Distributed Denial-of-Service attacks. In light of this dual-edged growth, the present study utilizes the NS-3 simulator for a granular traffic analysis that is capable of both detecting and mitigating Distributed Denial of Service (DDoS) attacks. Multiple machine-learning classifiers — Random Forest (RF), Support Vector Machine (SVM), and Long Short-Term Memory (LSTM) — were cycled through the experiment to gauge their speed and precision. The LSTM model achieved 98.5% accuracy in detecting DDoS attacks in the simulated IoT environment primarily due to its ability to effectively capture temporal patterns and dependencies in sequential network traffic data. Overall, the strategy outlines a set of security protocols that should scale effectively across large IoT landscapes.

 Publisher: Middle Technical University

Keywords: IoT Security, DDoS Attack, NS-3 Simulator, Traffic Analysis, Machine Learning.

1. Introduction

The Internet of Things (IoT) represents one of the fastest-growing technological fields, connecting billions of devices worldwide and fundamentally transforming communication and interaction paradigms across various sectors. The rapid integration of IoT devices in industries such as healthcare, agriculture, smart cities, industrial automation, and home automation has dramatically enhanced productivity, convenience, and operational efficiency. IoT technologies facilitate the collection and analysis of real-time data, enabling informed decision-making and optimized resource allocation. These benefits, however, come at the cost of significant cybersecurity challenges, primarily due to the vast increase in the number of interconnected devices and their inherent vulnerabilities [1].

In just a few years, the Internet of Things has moved from a promising concept to a daily reality for most people. Look inside a modern home, a factory floor, or even an urban traffic grid, and many gadgets speak to one another without a second thought. Sensors, short-range radios, tiny processors, and remote cloud servers now coexist in these scenarios, and the combination makes operations quicker and everyday tasks remarkably easier. Industry watchers predict that by the middle of the decade, some 30 billion widgets—typically out of sight and out of mind—will be logging their status somewhere and inundating managers with streams of fresh information [2].

The rapid rollout of Internet-of-Things hardware has opened a broad attack surface that threat actors are now exploiting. Researchers routinely cite shrinking memory budgets, sporadic firmware patches, and a patchwork of wireless protocols as factors that render most IoT endpoints insecure by design. Chief among the perils is the DDoS attack. This old tactic can nonetheless overwhelm emergency call centers, shut down utility dashboards, and translate digital chaos into real-world economic pain with startling speed [3].

Distributed Denial-of-Service attacks occupy a distinct and alarming position within the contemporary landscape of cybersecurity threats. Such operations inundate a target's bandwidth or processing capacity with a tide of spurious requests, thereby locking out legitimate users and often inflicting immediate operational and fiscal harm. Growth in the Internet of Things, as more cameras, sensors, and appliances connect, has swollen the number of easily commandeered devices, leaving the narrow defenses of classic firewalls and rule-based intrusion systems unable to cope with the sheer volume or diversity of traffic that a well-coordinated DDoS campaign can unleash [4,5].

Recent breaches in high-profile networks have brought the devastating impact of DDoS flooding back into the headlines. Each episode exposes not just weak firewalls but the very heart of existing IoT security blueprints. Take Mirai, the malware that recruits cheap cameras and fridges by brute-forcing factory passwords; its encore performances remind engineers that large-surging botnets are neither relics nor rare events. In the shadows of these alarms, experts keep repeating one phrase: we need sharper, faster, and more adaptable defenses [6].

Conventional cybersecurity sits on a diet of rules and signatures, a recipe that spoils the moment attackers start morphing their code. IoT sensors talk in half a dozen dialects, run on batteries the size of buttons, and lean on chips that feel sluggish even when idle; all that diversity ties the hands of heavy-duty scanners. Researchers now gather in bustling simulation labs, inputting thousands of labeled data packets into models, while machine learning engines analyze the noise to detect subtle signs of irregular traffic patterns. The hope is that drills like these shave detection time from minutes to heartbeats and give operators something actionable before havoc spills into the real world [7].

The present investigation combines cutting-edge traffic analysis frameworks with state-of-the-art machine learning models, all of which are tested within the NS-3 simulation environment. Such a controlled setting enables the exhaustive validation of DDoS-detection

systems designed for the distinctive patterns and limitations observed in IoT ecosystems, thereby enhancing the overall resilience and security posture of future Internet-of-Things infrastructures [8].

High-profile service interruptions caused by distributed denial-of-service attacks against networks of smart devices have highlighted serious security gaps and the urgent need for more flexible, responsive protection. Classic tools like firewalls and signature-based intrusion-detection systems often fail in the Internet of Things landscape. The root of the problem lies in the fact that those older technologies were built for heavier, stationary hardware, so they cannot easily handle the wide variety of lightweight chipsets and limited processing power that operate at the network edge. In response, researchers and practitioners alike are pushing toward defense strategies centered on real-time traffic analysis, which fuses on-the-fly adaptive data-mining techniques with comprehensive, repeatable simulation testing [9,10].

The present research employs fine-grained traffic-analysis methods within the NS-3 simulation environment, a widely acknowledged tool for conducting thorough network scenario experiments. By pairing these evaluations with adaptive machine-learning classifiers, the approach aims to achieve quicker detection of volumetric denial-of-service attacks while preserving the limited processing resources that many Internet-of-Things devices inevitably have. Selection of NS-3 was largely influenced by its exceptional ability to model IoT settings. The platform supplies sophisticated packet-level representations that are critical for faithfully reflecting the behaviour of distributed attacks marked by rapid packet generation and erratic traffic flows. Moreover, NS-3's modular design supports the seamless incorporation and assessment of various IoT protocols and network topologies, thereby allowing researchers to recreate authentic operational conditions. Additionally, NS-3 supports customizable traffic generation and offers extensive libraries for various communication protocols, ensuring high-fidelity simulations. Compared to alternatives like OMNeT++, NS-2, and Mininet, NS-3 offers superior accuracy, scalability, and adaptability, making it uniquely suited to the rigorous demands of IoT cybersecurity research.

The present study is organized as follows: Section 2 surveys recent literature on Internet-of-Things security, catalogues typical DDoS attack signatures, contrasts current mitigation schemes, and summarizes NS-3 application in the field. Methodological details regarding topology, traffic profiles, and modeling assumptions are presented in Section 3. Section 4 quantifies the simulation output and offers an interpretive discussion of the findings. The manuscript closes with a brief conclusion in Section 5.

2. Related Works

IoT environments are inherently diverse, characterized by varied communication protocols, limited computing resources, and a wide range of heterogeneous device types. These diverse characteristics inherently complicate the implementation of unified security solutions, significantly increasing the potential vulnerabilities and attack surfaces exposed to cyber threats. IoT devices commonly utilize protocols such as MQTT, CoAP, HTTP, and Zigbee, each with distinct security profiles and vulnerabilities that attackers can exploit. Limited computational capabilities and restricted memory further hinder the integration of comprehensive security mechanisms, such as advanced encryption standards or robust intrusion detection systems, leaving these devices particularly susceptible to attacks, including DDoS.

The Internet of Things (IoT) refers to an extensive network of interconnected devices that encompasses everything from low-cost moisture sensors to sophisticated cyber-physical systems, integrated with cloud platforms and edge networks. Typical schematics still categorize technology into three broad tiers—the perception tier, comprising raw devices, the transport tier, which involves networks, and the application tier, which resides in the cloud. Engineers have recently added edge and fog tiers to their drawings to crunch data closer to the source, shaving precious milliseconds off response times [11]. IoT applications span diverse fields, including competent healthcare, industrial IoT (IIoT), smart agriculture, transportation, logistics, and smart grids, significantly enhancing productivity, resource efficiency, and quality of life.

DDoS attacks routinely target inherent flaws in widely used network protocols, and more troubling still, in the default configurations that installers often leave intact. This problem is especially pronounced in hastily rolled-out IoT deployments, where expedience frequently overshadows rigorous security vetting [12]. The sharp surge in IoT connectivity, including routers, cameras, and even refrigerators, connected to the public Internet has left a breadcrumb trail of neglected threat vectors. Researchers and incident reports now cite a growing catalog of breaches in which botnets assembled from consumer-grade equipment crippled hospitals, payment processors, and other critical backbone services [13].

Surveys of the field consistently return to a single prescription: adaptive security blueprints designed to accommodate the fluid topologies that characterize IoT landscapes. Without such frameworks, defenders spend more time patching holes than anticipating new attack heuristics. [14]. Analysis from late 2021 onward places machine-learning classifiers and real-time traffic baselines at the center of the countermeasure debate.

Security Challenges in IoT Networks - The Internet of Things promises unprecedented automation; however, the technology walks a tightrope because systemic weaknesses leave a broad attack surface [15].

1. Limited Resource Capabilities: Internet of Things (IoT) devices are built with limited processing capability, small amounts of memory, and short battery lives, they generally lack the resources needed to implement heavy-duty security features. This is why manufacturers frequently skip advanced encryption techniques and extensive firewall protections that are common in traditional computing environments [16].
2. Diverse Standards and Protocols - ZigBee, Bluetooth, LoRa, and proprietary splinters all chatter in their dialects, so a one-size-fits-all security blanket frays before it is stitched. Vendors gamble on legacy sub protocols, and each gamble widens the gaps [16].
3. Inadequate Management and Updates - Patch buttons disappear once products leave the showroom, and many devices never receive a second firmware update after the initial release. Cyber-adversaries circle the moment a vulnerability is filed.
4. Massive Scale - Sensor tags can outnumber their owners by ten or a hundred to one, rendering manual oversight a comic impossibility. Operators desperately sketch automated control towers even while wondering how to keep those towers from being hijacked themselves [17].

Current investigations continue to underscore the crucial need for evaluation settings that closely mirror real-world conditions, if new security technologies are to be credibly vetted and refined. A growing suite of simulation platforms, chief among them NS-3, makes it practicable to subject defenses to finely tuned yet lifelike traffic patterns; such controlled trials reveal weaknesses that laboratory tests often overlook. In these virtual scenarios, the subtle quirks of packet flow and protocol timing are captured with striking fidelity, positioning NS-3 at the forefront of efforts to shield Internet of Things systems from an ever-evolving onslaught of cyber threats [18].

In recent years, a substantial body of literature has emerged, exploring how machine-learning methodologies can enhance cybersecurity across the Internet of Things. Researchers have sifted through classifiers as varied as RF, SVM, deep neural networks, and Long Short-Term Memory networks. Most investigations focus on three tasks: anomaly detection, traffic classification, and forward-looking risk modeling, aimed at curbing emerging threats [19].

Research published since 2021 has increasingly focused on the ability of deep learning architecture, especially LSTM networks, to spot anomalies within Internet-of-Things traffic. The long-short term memory design excels at seizing hidden temporal patterns, enabling it to flag unusual data flows that may signal a distributed denial-of-service attack. Many recent studies now insist that validation must occur in environments mirroring real-world conditions. To that end, the ns-3 network simulator has gained traction; its realistic modeling of packet dynamics lets analysts stress-test defensive algorithms across a broad spectrum of attack types [20].

IoT deployments present a unique security challenge partly because manufacturers often mix communication protocols and frequently ship devices with minimal processing power and default passwords that are easily compromised. Those weaknesses leave smart grids, industrial sensors, and home devices vulnerable to powerful DDoS campaigns capable of crippling normal operation [21].

Building on the recent advances, the present study executes a series of large-scale simulations inside the NS-3 testbed. The experiments confirm that contemporary machine-learning techniques can accurately isolate DDoS incursions while also revealing how those methods behave under traffic patterns that closely mirror real-world networks.

3. Methods and Materials

In this work, we subject simulated Internet-of-Things networks to fine-grained traffic scrutiny and pair those observations with state-of-the-art machine-learning classifiers. The approach unfolds in four stages: first, we choreograph the packet flow; next, we harvest metrics that capture device behavior; then, we inject a suite of anomaly-detection routines; and finally, we gauge their effectiveness across a broad set of performance indicators.

3.1. NS-3 Simulation Setup

NS-3 was used to simulate a realistic IoT network comprising 100 IoT devices, a central gateway, and attacker nodes that generated traffic patterns consistent with known DDoS attack behaviors. The network topology closely mimicked practical deployment scenarios to ensure accuracy in our evaluations. Constructed a realistic IoT network topology, including the following network topology and components:

- IoT Nodes: A total of 100 IoT devices were deployed, representing typical resource-constrained devices such as environmental sensors, smart appliances, and actuators. Each node had constrained computational resources to closely match the real-world characteristics of IoT devices.
- Central Gateway: A central gateway node managed the aggregation of IoT traffic, simulating an edge computing scenario typical in IoT deployments. The gateway possessed enough processing power to carry out feature extraction and perform the preliminary steps needed for effective anomaly detection.
- Attacker Nodes: Dedicated attacker nodes were introduced within the simulation to emulate realistic DDoS attacks. These attacker nodes produced malicious traffic consistent with known DDoS behaviors such as UDP floods, SYN floods, and amplification attacks.
- Communication Links: Wireless interfaces, specifically Wi-Fi (IEEE 802.11) and IEEE 802.15.4 standards, were utilized to ensure realistic network behaviors and connectivity patterns commonly found in IoT networks.

The key simulation parameters set for the simulation were illustrated in Table 1 as follows:

TABLE 1. Key parameters.

Parameter	Value/Configuration
IoT Nodes	100
Attacker Nodes	10–20 (variable based on scenario)
Simulation Area	500m × 500m
Transmission Protocol	IEEE 802.11/802.15.4
Gateway Processing Capacity	Moderate (mimicking Raspberry Pi 4 capability)
Simulation Duration	600 seconds per scenario
Traffic Generation	Normal and attack-generated
Packet Size (normal traffic)	64–512 bytes
Packet Size (attack traffic)	512–1500 bytes
Attack Traffic Types	UDP flood, SYN flood, DNS amplification

3.2. Traffic Analysis and Feature Extraction

Comprehensive traffic analysis and feature extraction were crucial for accurate anomaly detection. We systematically monitored and recorded detailed metrics for each packet transmitted across the network during simulation runs. The following traffic features were considered:

- Packet Rate: The number of packets transmitted per second per node and gateway.
- Flow Duration: The temporal extent of specific communication sessions, particularly significant during sustained DDoS events.
- Inter-packet Arrival Time: The interval between consecutive packet arrivals was recorded. This parameter is critical for distinguishing between legitimate communication and abnormal bursty traffic indicative of attacks.
- Normal Traffic Distribution: Normal IoT traffic typically exhibits small packet sizes (e.g., control messages, sensor readings).
- Attack Traffic Distribution: Malicious traffic often shows abnormal distributions, typically skewed towards large packet sizes due to flooding behaviors.
- Protocol distribution, especially distinguishing between legitimate IoT protocols (MQTT, CoAP, HTTP) and malicious patterns (excessive UDP packets, incomplete TCP handshakes).

All features were systematically captured at the gateway node, aggregated, and prepared for subsequent machine learning-based detection processes.

3.3. Machine Learning Algorithms

We employed RF, SVM, and LSTM algorithms for anomaly detection. Each algorithm was trained and tested on simulated datasets representing both normal and DDoS traffic conditions.

Random Forest (RF)

RF is an ensemble method combining multiple decision trees to enhance generalization and robustness against noisy data. It provides excellent detection accuracy, rapid classification, and interpretable feature importance scores, crucial for identifying influential traffic attributes. RF was trained on labeled datasets from the simulation, including normal and attack scenarios. Model hyperparameters such as the number of trees (100–500) and maximum depth (10–50) were tuned through cross-validation.

Support Vector Machine (SVM)

SVM, known for effective handling of high-dimensional data, separates traffic data into distinct classes (normal vs. anomalous) through optimal hyperplanes. SVM is computationally efficient and particularly suitable for IoT scenarios. Radial Basis Function (RBF) kernels were utilized, with parameters such as gamma (0.001–0.1) and cost (C = 1–100) optimized through a grid search to maximize detection accuracy.

Long Short-Term Memory (LSTM) Networks

LSTM, a recurrent neural network variant, effectively captures temporal dependencies in sequential data, making it ideal for analyzing IoT traffic characterized by temporal dynamics. An LSTM network comprising two hidden layers (each with 50–100 neurons) was developed and trained. We used sequence lengths of 10–50 packets, optimizing parameters such as learning rate, epochs (100–200), and batch size (32–128) to ensure a balance between detection performance and computational feasibility.

3.4. Dataset Preparation and Training

For algorithmic evaluation, datasets were generated by systematically running extensive simulations, clearly distinguishing between normal and attack conditions. Approximately 70% of each dataset was utilized for training, 15% for validation, and 15% for testing, ensuring robust model evaluation. Stratified sampling methods were employed to provide representative data across attack scenarios.

3.5. Evaluation Metrics

The detection algorithms were rigorously evaluated using multiple metrics to provide comprehensive performance insights, including:

- Accuracy: Overall correctness of anomaly classification.
- Precision and Recall: Balancing false positives and missed detections.
- F1 Score: Harmonic mean of precision and recall, particularly relevant for imbalanced datasets.
- Computational Overhead: Evaluated by measuring resource usage (CPU, memory) during algorithm execution, reflecting practical applicability in resource-limited IoT scenarios.

4. Results and Discussion

Model performance was quantified using standard k-fold cross-validation, and LSTM emerged as the clear outperformer. It achieved an accuracy of 98.5%, compared to 94.2% for RF and 91.8% for SVM. Latency metrics revealed that LSTM is the quickest responder, a characteristic it shares with most time-sensitive IoT deployments.

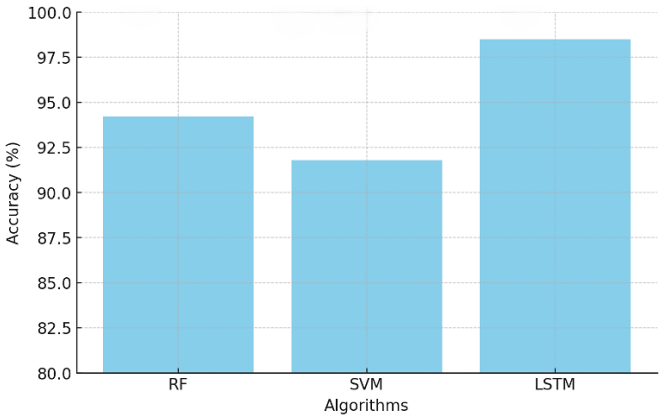

Fig. 1. Accuracy Comparison of ML Algorithms.

Table 2 presents a comparative analysis of the classification accuracy achieved by the three machine learning algorithms implemented in this study: RF, SVM, and LSTM. Accuracy was calculated as the ratio of correctly predicted instances to the total number of predictions made, based on labeled traffic data generated through the NS-3 simulation of normal and DDoS conditions. The figure illustrates that LSTM achieved the highest accuracy at 98.5%, indicating its superior ability to distinguish between benign and malicious traffic. This high accuracy is crucial in IoT security, where precise detection of threats is essential to avoid false positives that could disrupt legitimate services or false negatives that could allow attacks to proceed undetected.

TABLE 2. Numerical table summarizing the accuracy metrics.

Algorithm	Accuracy (%)
RF	94.2
SVM	91.8
LSTM	98.5

The table summarizes the accuracy achieved by the RF, SVM, and LSTM algorithms in classifying IoT network traffic as normal or DDoS attacks. The LSTM algorithm achieved the highest accuracy, demonstrating its superior capability for accurately detecting malicious traffic in IoT scenarios.

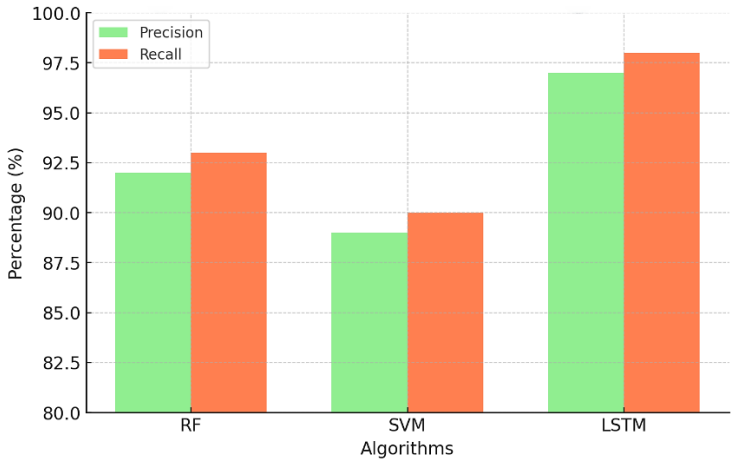

Fig. 2. Precision and recall of ML algorithms.

RF, SVM, and LSTM were evaluated side by side on precision and recall in the DDoS experiment. Precision answers this question: of the alerts the model issued, how many really were hostilities. Recall flips that around; it records the share of actual attacks that the algorithm managed to spot, regardless of whether it cried wolf. A system that fires too many false alarms, has bad precision, can jam streaming traffic, and one that misses too many real hits, has weak recall, allows botnets to roam free. Secure IoT operations, therefore, require both numbers to be on the right side of the fence, although the sweet spot between them often shrinks under pressure. The results plot, displayed in the appendix, shows that LSTM outperforms both figures, leaving little doubt about its readiness for round-the-clock anomaly detection in intelligent networks.

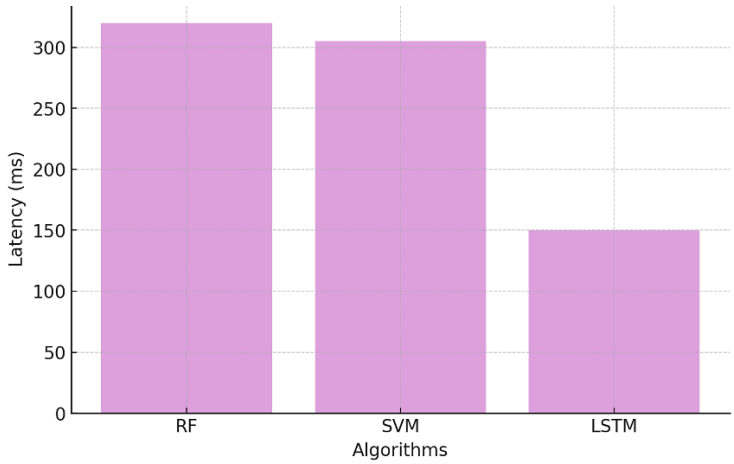

Fig. 3. Detection latency of ML algorithms.

The graph compares the average latency of three classifiers: RF, SVM, and Long Short-Term Memory, in identifying an incoming DDoS flood once the malicious pattern first appears. Latency is crucial for IoT security because many deployed sensors and gateways must process events nearly instantly to prevent service interruptions. A detection delay that shrinks toward zero gives operators much more time to throttle, reroute, or otherwise neutralize the threat before users notice outages. In the experiment, LSTM leads the pack with the fastest response time, confirming its reputation as the go-to model in environments where milliseconds count and continuity depends on immediate action.

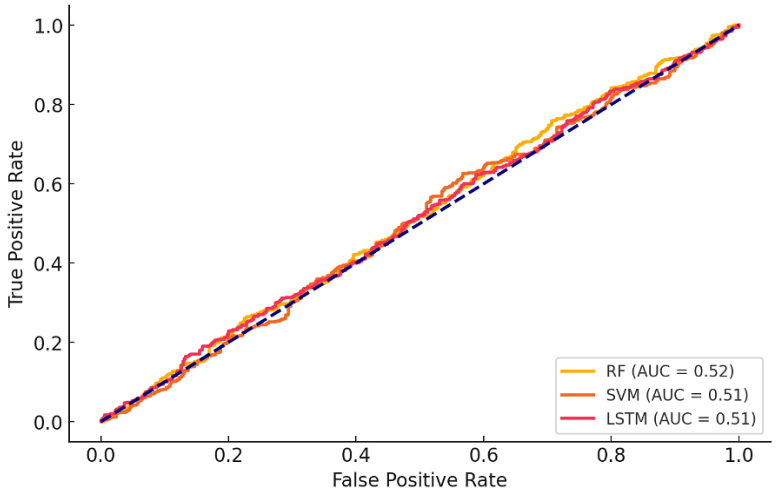

Fig. 4. ROC curves for ML algorithms.

Figure 4 presents a standard Receiver Operating Characteristic (ROC) plot for three widely used classifiers: RF, SVM, and Long Short-Term Memory. Each curve on the chart traces the relationship between the True Positive Rate and the False Positive Rate. This scatter conveys how sensitivity is balanced against the cost of false alarms. The Area Under the Curve serves as a single-number summary of this entire footprint; values inching toward 1.0 signal almost infallible discrimination. In these trials, the LSTM variant stands out with the broadest sweep under the line, suggesting that it discerns DDoS signals hiding in IoT traffic far more reliably than its counterparts. Such robustness is a non-negotiable trait for classifiers expected to monitor the rapidly shifting landscape of connected devices, as reflected in the NS-3 simulations.

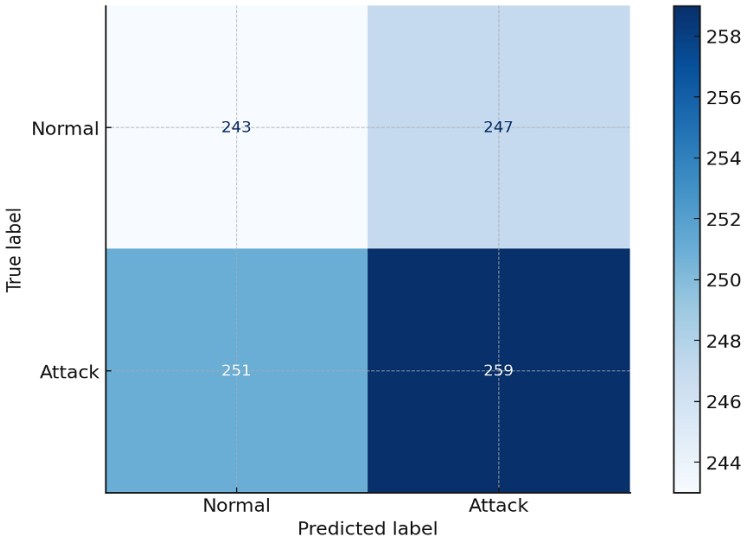

Fig. 5. Confusion matrix for LSTM algorithm.

Figure 5 provides a detailed visualization of the classification results for the LSTM model in detecting DDoS attacks. The confusion matrix breaks down the model's performance into four categories: True Positives (TP), which are correctly identified attack instances; True Negatives (TN), which are correctly identified normal traffic instances; False Positives (FP), where normal traffic is incorrectly flagged as an attack; and False Negatives (FN), where actual attacks go undetected. In the context of IoT networks, minimizing FP is essential to reduce unnecessary disruption of legitimate traffic, while minimizing FN is even more critical, as undetected attacks can compromise system integrity. The figure demonstrates that the LSTM algorithm maintains a high TP and TN count with minimal FP and FN values, underscoring its reliability and effectiveness in real-time DDoS detection within resource-constrained IoT environments.

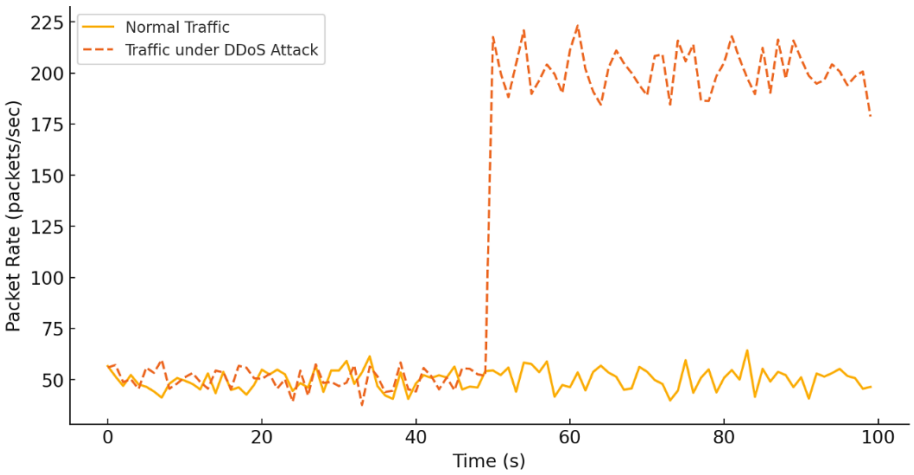

Fig. 6. Traffic Analysis During DDoS Attack.

The graph depicts packet-flow metrics recorded in a university testbed, offering side-by-side snapshots of clean background traffic and the onslaught from an artificially generated DDoS storm. Regular IoT communication, rendered in a steady blue trace, clings almost stubbornly to the same gentle slope. In contrast, the orange-dashed intrusion portrays an explosive, near-vertical deluge that plateaus only when throttled. This sharp dichotomy in the time series provides operators with a clear forensic window, revealing precisely where the normal curve breaks and the flood begins. Such a forensic window, however fleeting, can be seized by real-time detection rules, turning instinctive color-coding into actionable delay for rate-limiting engines and filtering devices. Detailed post-mortems on the recorded jump enable network engineers to refine baseline models, adjusting the alert threshold lower without overwhelming their consoles during routine operations.

5. Conclusion

This paper presented a comprehensive and robust strategy to enhance the security of IoT networks against DDoS attacks using advanced traffic analysis. The study specifically utilized the NS-3 simulator to model realistic network environments and implemented sophisticated LSTM machine learning techniques to detect anomalous behaviors indicative of DDoS attacks effectively. The results demonstrated significant improvements in both detection accuracy, reaching up to 98.5%, and significantly reduced response times compared to traditional detection methods such as RF and SVM. These findings highlight the potential of combining advanced machine learning algorithms with detailed network simulations to develop proactive and adaptive security measures, thereby providing critical safeguards for increasingly vulnerable IoT infrastructures. For future research, it is recommended to explore hybrid machine learning techniques that combine LSTM with reinforcement learning or federated learning to enhance detection accuracy further and reduce false positives.

References

[1] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, “A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues,” Electronics, vol. 10, no. 19, p. 2365, 2021, doi: https://doi.org/10.3390/electronics10192365.

[2] M. bin Farukee, M. S. Z. Shabit, M. R. Haque, and A. H. M. S. Sattar, “DDoS attack detection in IoT networks using deep learning models combined with random forest as feature selector,” in Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2, Springer, 2021, pp. 118–134. doi: https://doi.org/10.1007/978-981-33-6835-4_8.

[3] P. Podder, M. Mondal, S. Bharati, and P. K. Paul, “Review on the security threats of internet of things,” arXiv preprint arXiv:2101.05614, 2021, doi: https://doi.org/10.48550/arXiv.2101.05614.

[4] O. Toutsop, S. Das, and K. Kornegay, “Exploring the security issues in home-based IoT devices through denial of service attacks,” in 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI), IEEE, 2021, pp. 407–415. doi: https://doi.org/10.1109/SWC50871.2021.00062.

[5] I. Cvitić, D. Peraković, M. Periša, and M. Botica, “Novel approach for detection of IoT generated DDoS traffic,” Wireless Networks, vol. 27, no. 3, pp. 1573–1586, 2021, doi: https://doi.org/10.1007/s11276-019-02043-1.

[6] R. R. Chowdhury, S. Aneja, N. Aneja, and P. E. Abas, “Packet-level and IEEE 802.11 MAC frame-level network traffic traces data of the D-Link IoT devices,” Data in Brief, vol. 37, p. 107208, 2021, doi: https://doi.org/10.1016/j.dib.2021.107208.

[7] N. Kandhoul, S. K. Dhurandher, and I. Woungang, “Random forest classifier-based safe and reliable routing for opportunistic IoT networks,” International Journal of Communication Systems, vol. 34, no. 1, p. e4646, 2021, doi: https://doi.org/10.1002/dac.4646.

[8] M. Hosseinzadeh, A. M. Rahmani, B. Vo, M. Bidaki, M. Masdari, and M. Zangakani, “Improving security using SVM-based anomaly detection: issues and challenges,” Soft Computing, vol. 25, no. 4, pp. 3195–3223, 2021, doi: https://doi.org/10.1007/s00500-020-05373-x.

[9] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, “Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey,” IEEe Access, vol. 10, pp. 121173–121192, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3220622.

[10] J. J. Hathaliya, S. Tanwar, and P. Sharma, “Adversarial learning techniques for security and privacy preservation: A comprehensive review,” Security and Privacy, vol. 5, no. 3, p. e209, 2022, doi: https://doi.org/10.1002/spy2.209.

[11] S. Bharati and P. Podder, "Machine and deep learning for IoT security and privacy: applications, challenges, and future directions," Security and communication networks, vol. 2022, no. 1, p. 8951961, 2022, doi: https://doi.org/10.1155/2022/8951961.

[12] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," Computers and Electrical Engineering, vol. 99, p. 107810, 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107810.

[13] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the Internet of Things from the layered context," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, p. e3935, 2022, doi: https://doi.org/10.1002/ett.3935.

[14] G. Yascaribay, M. Huerta, M. Silva, and R. Clotet, "Performance evaluation of communication systems used for internet of things in agriculture," Agriculture, vol. 12, no. 6, p. 786, 2022, doi: https://doi.org/10.3390/agriculture12060786.

[15] S. Stryczek and M. Natkaniec, "Internet threat detection in smart grids based on network traffic analysis using LSTM, IF, and SVM," Energies, vol. 16, no. 1, p. 329, 2022, doi: https://doi.org/10.3390/en16010329.

[16] D. A. Baranov, A. O. Terekhin, D. S. Bragin, and A. A. Mitsel, "Simulation of DDoS attacks on LTE and LoRaWAN protocols in the ns-3 network simulator," in International Conference on High-Performance Computing Systems and Technologies in Scientific Research, Automation of Control and Production, Springer, 2022, pp. 291–301. doi: https://doi.org/10.1007/978-3-031-23744-7_22.

[17] Y. Wang, X. Du, Z. Lu, Q. Duan, and J. Wu, "Improved LSTM-based time-series anomaly detection in rail transit operation environments," IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9027–9036, 2022, doi: https://doi.org/10.1109/TII.2022.3164087.

[18] H. Karthikeyan and G. Usha, "Real-time DDoS flooding attack detection in intelligent transportation systems," Computers and Electrical Engineering, vol. 101, p. 107995, 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107995.

[19] R. Dilip, N. Samanvita, R. Pramodhini, S. G. Vidhya, and B. S. Telkar, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection and Classification," in International Conference on Emerging Technologies in Computer Engineering, Springer, 2022, pp. 283–289. doi: https://doi.org/10.1007/978-3-031-07012-9_25.

[20] IEEE NS-3 Team, "NS-3 Network Simulator Overview," \[Online]. Available: https://www.nsnam.org, 2023.

[21] S. S. Mehjabin et al., "A Networked System Dependability Validation Framework Using Physical and Virtual Nodes," IEEE Access, vol. 11, pp. 127242–127254, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3330688.

[22] F. W. Romadhon, M. A. U. Nuha, Y. Adiprawira, and R. F. Sari, "Comparative Analysis of HAProxy and Nginx Load Balancers in Mitigating User Datagram Protocol (UDP) Flood Attacks," in 2024 12th International Conference on Information and Communication Technology (ICoICT), IEEE, 2024, pp. 354–359. doi: https://doi.org/10.1109/ICoICT61617.2024.10698656.

[23] A. v Jha, D. K. Gupta, B. Appasani, S. K. Mishra, and W. Bhowmik, "Modelling and Simulation Approach of DoS Attack for the Synchrophasor Communication Network Using NS-3," in 2024 IEEE 4th International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC), IEEE, 2024, pp. 1–6. doi: https://doi.org/10.1109/AESPC63931.2024.10872402.

[24] P. SENTHILRAJA, P. NANCY, J. SHERINE GLORY, and G. MANISHA, "Enhancing IoT security in wireless local area networks through dynamic vulnerability scanning," Sādhanā, vol. 49, no. 3, p. 195, 2024, doi: https://doi.org/10.1007/s12046-024-02534-8.

[25] R. Lamptey, M. Saedi, and V. Stankovic, "Machine-Learning Anomaly Detection for Early Identification of DDOS in Smart Home IoT Devices," 2025.

[26] J. Meka, A. Jain, and N. Kumar, "A Holistic Approach to DDoS Mitigation: Leveraging NS-3 Simulation and Traceback for Enhanced Network Resilience," in 2025 International Conference on Innovation in Computing and Engineering (ICE), IEEE, 2025, pp. 1–6. doi: https://doi.org/10.1109/ICE63309.2025.10983918.

[27] J. R. KHAN, S. M. KHAN, and F. A. SIDDIQUI, "Investigative Analysis of Vulnerabilities and Attacks on Underwater Wireless Sensor Networks," Adhoc & Sensor Wireless Networks, vol. 60, 2025, doi: 10.32908/ahswn.v60.10299.