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 grown quickly in the last few years, adding new features to everyday devices while also making those systems more vulnerable to more advanced Distributed Denial-of-Service attacks. Because of this two-sided growth, the current study uses the NS-3 simulator for a detailed traffic analysis that can find and stop DDoS attacks. The experiment used several machine-learning classifiers, including Random Forest, Support Vector Machine, and Long Short-Term Memory, to see how fast and accurate they were. The LSTM (Long Short-Term Memory) model was able to find DDoS attacks in the simulated IoT environment with 98.5% accuracy. This was mostly because it could accurately capture temporal patterns and dependencies in sequential network traffic data. The strategy as a whole lays out a set of security rules that should work well across large IoT networks.

 Publisher: Middle Technical University

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

1. Introduction

The Internet of Things (IoT) is a field of technology that is growing very quickly. It links billions of devices all over the world and changes how people talk to each other and work together in many areas. Connected devices such as in health care, agriculture, smart cities, industrial automation, and even home automation, have become common IoT applications that greatly enhance productivity, ease and effectiveness of their respective operations. IoT technologies enable these systems to gather and interpret data instantaneously. This functionality facilitates well-informed decision making and judicious allocation and use of resources. However, IoT devices have immense cybersecurity challenges given the shear increase and inherent vulnerabilities of the connected devices [1].

The Internet of Things has gone from a promising idea to a part of everyday life for most people in just a few years. Many gadgets talk to each other without even thinking about it in a modern home, on a factory floor, or even in a city traffic grid. In these situations, sensors, short-range radios, tiny processors, and remote cloud servers all work together. This speeds up operations and makes everyday tasks much easier. By the middle of the decade, some 30 billion widgets—most of which are out of sight and out of mind—will be keeping track of their status somewhere and sending managers streams of new information [2].

Threat actors are now taking advantage of the wide range of attack surfaces that have opened up because of the quick rollout of Internet of Things hardware. Researchers often say that most IoT endpoints are insecure by design because of things like shrinking memory budgets, sporadic firmware patches, and a patchwork of wireless protocols. The Distributed Denial of Service (DDoS) attack is the most dangerous of all. This old trick can still quickly overwhelm emergency call centers, shut down utility dashboards, and turn digital chaos into real-world economic pain [3].

At present, the distributed denial-of-service attacks (DDoS) hold a unique and alarming position. DDoS attacks work by filling the target's bandwidth or processing a stream of fake requests, thereby blocking servers. Any remaining requests are marked as collateral, and the target company, once again, faces the deepest consequences. Companies like D-Gate and other sensors are constantly adding new DDoS attack vectors as the IoT ecosystem continues to evolve. The size of the attack simply exceeds the capabilities of conventional firewalls as well as rule-based intrusion detection systems [4,5].

The recent cyber attacks on well known industries have shown in particular how weaknesses in DDoS flooding have become worse. Each case not only captures the outdated nature of the firewalls, but equally the incompetence of the protective mechanisms in use today for the Internet of Things. Mirai is a piece of malware that employs brute force attacks against cheap grade routers, cameras, and even fridges. Her repeat performances makes engineers feel that massive botnets are neither a thing of the past nor are they rare sights. Time and time again the specialists say the same thing, cloaked beneath the blaring of these sirens, lack of defenses that are more complex and advanced and far quicker and more flexible [6].

Attackers modify their codes which render rules and signatures useless and this is still referred to as traditional cybersecurity. It's difficult to work with heavy-duty scanners due to batteries the size of buttons and chips that are mechanically inactive IoT sensors speak 6 languages and. Collectively, they work at a pace that feels agonizingly slow. Researchers have turned their attention to busy simulation

labs, concentrating their efforts there. They teach their systems packets that have been labeled and classified. Simultaneously, machine learning systems are attempting to extract meaning from the bulk of the data, and scanning for minor fluctuations in the traffic which would be considered as the sign of the arrival of something important. The objective is for exercises like these to reduce the time needed for detection from a full 60 seconds down to a simple heartbeat, and, in the process, provide the operators with an activity to do before the actual mayhem breaks loose in the real world [7].

During the configuration of the NS-3 system , the innovation reaches new limits as new methods of traffic analysis and dynamic machine learning are combined. This further enhances the security and integrity of IoTs of the next generation. It allows the detailed design and analysis of the DDoS detection system for the peculiar and sophisticated behaviors of IoT systems [8].

The recent attacks on smart device networks that have resulted in service outages demonstrate primary security issues that need to be defended against in a flexible and timely manner. A DDoS attack in IoT relies on older technologies such as supported by a firewall and signature-based intrusion-detection systems that have little efficacy. The issue is that such older technologies mapped to technological infrastructure and support legacy which is still cumbersome and rigid and thus, unable to deal with low power chipsets and edge-of-network processing. There is a growing agreement among researchers and practitioners on the need to develop and adopt defense strategies that consider real-time analytics on traffic streams. These would fuse real-time pattern recognition and data mining with powerful numerical simulation models to craft new technologies [9,10].

This study employs fine-grained traffic analysis within the NS-3 environment which is considered a dependable method for carrying out complex and repeatitive network analysis. The framework is designed for modeling volumetric Distributed Denial-of-Service (DDoS) attacks using adaptive machine learning classifiers for realtime computation. The methodology achieves the equilibrium between machine learning processes and the operational efficiency required for low power IoT devices. NS-3 serves the purpose of analyzing packet level behaviors for IoT and the provided framework helps in understanding the DDoS attack and the random burst and erratic flow patterns the attack creates. Modular design of NS-3 offers easy integration for swift testing of varioud IoT communication protocols coupled with network topologies for useful setting replication. NS-3's extensive, dynamically adjustable, self-contained protocol libraries and traffic generation tools for coherent design and seamless testing facilitates precise, flexible, and real-time analysis. Relative to competing simulation tools OMNeT++, NS-2, and Mininet, NS-3 outperforms them in providing finer simulations, greater user capacity, and more versatility in tailored modifications for operational requirements. This in turns facilitates the analysis of real IoT systems by studying the interplay of the components within the IoT security architectures for systems.

The structure of the paper is as follows. In Section 2, the most recent information concerning security issues in the Internet-of-Things is reviewed, and the characteristic signatures of DDoS attacks are compiled and attempts at mitigation are analyzed and an overview of the NS-3 is provided. In Section 3, the methods used to develop the topology, traffic profiles, and the model's assumptions are described. In Section 4, the output of the simulation is analyzed and discussed in a sensible manner. The paper is finalized in Section 5, in which the principal points are briefly discussed.

2. Related Works

Due to varying communication protocols, different computing capabilities, and the many types of devices that work differently, IoT environments tend to be heterogeneous in nature. Such traits and characteristics make the implementation of unified security solutions more difficult. In the same light, unified security solutions make robust protections more difficult, thereby increasing the chances of a cyber attack. IoT devices overwhelmingly utilize MQTT, CoAP, HTTP, and Zigbee protocols. Each protocol has its own set of vulnerabilities and security weaknesses. Due to these traits, more advanced security features are difficult to implement, such as strong intrusion detection systems and advanced encryption standards. Such features make devices in the IoT sphere more likely to be attacked by a Distributed Denial of Service (DDoS) attack.

The Internet of Things refers to an expansive network of interconnected objects that encompasses everything from basic sensors and devices to sophisticated cyber-physical systems interfacing with the cloud and edge networks. Most conventional diagrams still allocate technology to three overarching tiers: the perception tier which includes all devices on the ‘edge’, the transport tier which consists of networks, and the application tier which resides in the cloud. More recently, engineers have started incorporating edge and fog tiers into their diagrams to perform real-time data processing and reduce latency by valuable milliseconds [11]. The applications of the Internet of Things encompass areas like smart agriculture, smart transportation and logistics systems, and smart grids. The use of these technologies leads to an increase in productivity, optimal use of resources, and an improved quality of life. DDoS assaults frequently pinpoint the fundamental design weaknesses of widely-used network protocols and, more alarmingly, they tend to focus on the ‘out of the box’ configurations that users tend to neglect. This issue is particularly exacerbated in the domain of the Internet of Things, where systems are haphazardly integrated, and systems where, more often than not, the need for a comprehensive security assessment is sacrificed for the need for speed [12]. The alarming number of Internet of Things devices connecting to the public Internet without any form of configuration or security, such as routers, video cameras, or even smart refrigrators, gives rise to numerous unaddressed security issues. Such devices have become the part of botnets that are taking down critical services such as hospitals and payment processing systems, and these cases are becoming part of the lore in the security community [13].

The literature in the area has yet to come up with any new concepts. It still suggests working on “adaptive security more than any other theme. Without such paradigms, the defense is more reactive, and trying to guess the paradigms of unanticipated new attacks.” [14]. Since the end of 2021, the discussions of the countermeasure debates have focused mostly on the machine-learning classifiers and real-time traffic baselines.

Issues with IoT networks security – the Internet of Things offers levels of automation unparalleled to ever before, however, due to the intrinsic vulnerabilities, the technology rests on thin ice, and is prone to imminent attacks [15].

1. Resource Constraints: The lack of significant processing capacity, memory, and battery life means that IoT devices will be unable to employ more robust security functionalities, and this is the reason why manufacturers often do not implement high-grade encryption or strong firewall defenses that are characteristic of the conventional computing space [16].
2. Different frameworks and standards – ZigBee, Bluetooth, LoRa and proprietary splinters – all correspond in their own dialects. Thus, a blanket of security rhetoric comes apart at the seams before it is fully originated. Vendors take risks on outdated sub protools, and with each new gamble, the fissures in the fabric grow [16].
3. Lack of proactive management and developmental lags: Unexplained gaps in the stepwise elbow and squeak the show and the inability to deliver two entire firmware updates for a slew of devices after the first one. The second a weakness in a system is uncovered, dark web operatives begin.

4. The Quantities of Sensor Tags: The possession of sensor tags ranges from a minimum of 10 to a maximum of 100 per person. Hence, it becomes physically impractical to keep track of all of them. As the designers of these systems attempts to solve the question of how to rein in the hijacking of these control towers, the systems themselves are being rapidly constructed [17].

The effectiveness of scenario strategy based evaluation in the development and testing of advanced security tools is especially relevant in light of recent findings. There is an increasing suite of simulation tools, the most well-known of which is NS-3, which constructs simulated environments for the application of defenses to sanitized clouds of realistic traffic. These simulations, which are beyond what has been attainable in laboratory contexts, expose gaps in defense stratagems. In these scaled simulations, NS-3 captures the envelope of the problem space, calculating packet dynamics and control interlaced protocol timing with phenomenal levels of fidelity. This is what distinguishes NS-3 in the defense perimeters which are closing on an increasing number of sophisticated attacks on Internet of Things systems [18].

A significant body of literature has recently developed, examining the ways in which machine-learning methodologies can improve cybersecurity within the Internet of Things. Scientists have looked at a wide range of classifiers, including Long Short-Term Memory networks, deep neural networks, Support Vector Machines, and Random Forest. Most studies focus on three things: finding unusual behavior, classifying traffic, and making predictions about future risks in order to stop new threats [19].

Since 2021, an increasing amount of study has been done on how deep learning architectures, especially LSTM networks, are capable of discovering strange patterns in Internet-of-Things traffic. The long-short term memory design is great at finding hidden patterns in time, which lets it flag strange data flows that could be indicative of a distributed denial-of-service attack. Numerous recent studies now assert that validation must transpire in environments that replicate real-world conditions. The ns-3 network simulator has become popular for this reason: it lets analysts stress-test defensive algorithms against a wide range of attack types by realistically modeling packet dynamics [20].

The reason that IoT deployments are particularly weak in security is the attack systems having weak configured processing units that require the hand of the manufacturer in completing varied conversation protocols, along with having readily guessable defualt pesword systems. These flaws permit the easy DDoS attack array to cascade on big DDoS smarts, sensor grids and domestic units which disrupt the standard functioning of the systems [21].

The current work deepens recent advances by conducting a set of simulations at scale in the NS-3 testbed. The results from the experiments show on the one hand the capability of contemporary machine learning methodologies to effectively target DDoS attacks, while on the other hand demonstrating their behavior in traffic models that mimic real life networking systems.

3. Methods and Materials

This work partitions the analysis of extensive traffic studies on the simulated Internet of Things networks and their interfaces with advanced Machine Learning classifiers onto four steps. First, we design the packet routes. Second, we assess the device-level performance metrics. Third, we conduct behavioral anomaly detection and subsequent classification. In the last step, we evaluate the framework with respect to a diverse set of performance metrics.

3.1 NS-3 Simulation Setup

With the network simulator ns-3, we constructed an Internet of Things scenario with 100 IoT devices, a central gateway, and two attacker nodes simulating traffic patterns of known DDoS attacks. To satisfy the rigor of the evaluation, we constructed the network topology using an actual deployment case. Topology of an IoT network which consisted of:

• IoT Nodes: Each of the one hundred IoT devices was a real device that had real limitations, such as smart home devices, environmental monitoring devices, and control devices. Each of the nodes was built with the same level of computing technology constraints as smart IoT devices are in real life.

• Central Gateway: This central gateway node synthesized IoT traffic and was able to do so at the ‘edge’ of the IoT deployment. The gateway was strong enough to do a preliminary feature extraction and had enough computing power to carry out the first few crucial steps of successful anomaly detection.

• Attacker Nodes: In order to better the simulation of the DDoS attacks, specific nodes for DDoS attacks were added to the simulation. These avatars generated DDoS attack traffic which included UDP flood attacks, SYN flood attacks, and various amplification attacks.

• Supporting the previously mentioned observations of interactions of IoT networks and performing behavioral studies with respect to the elements of the topology of the network utilized physical communication interfaces, such as Wi-Fi (IEEE 802.11) and the standard IEEE 802.15.4.

The key parameters set for the simulation were 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

Anomaly detection relies on uninterrupted traffic analysis and feature extraction. During simulation runs, we meticulously captured and calculated intricate parameters for all network transmission packets. These are the underlying traffic parameters captured:

- 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

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)

Constructed using an ensemble methodology, Random Forest combines a set of decision trees to enhance generalization and protect the data from noise. Additionally, it performs exceptionally well in various data accuracy and speed classification, and provides an interpretable importance score which is vital in identifying the most relevant features of the traffic stream.

• Training and Evaluation: RF was trained using datasets obtained from the simulation with both normal and attack scenarios, which were appropriately labeled. Cross-validation was used to tune model hyper-parameters like the number of trees (100-500) and max depth (10-50).

Support Vector Machine (SVM)

SVM appropriately manages high-dimensional data by splitting the traffic data into two classes: normal and anomalous, using the most appropriate hyperplanes. SVM is also and therefore, advantageous in IoT settings.

• Kernel and Parameter Tuning. Tuning RBF kernels with gamma from 0.001-0.1 and range cost C = 1-100 was set in a grid search to optimize detection effectiveness.

Long Short-Term Memory (LSTM) Networks

An LSTM model is a specific type of recurrent neural network that specializes in understanding the interrelations of time ordered sequences, thus particularly applicable to the analysis of time-varying phenomena, such as IoT traffic.

• Architecture and Training: In designing an LSTM network model to be used for this specific inquiry, a two hidden layer LSTM network model was developed for which each hidden layer contained a specific 50 or 100 neuron architecture. The sequence lengths of the packets that made up the neural clusters were constrained to ranges between ten and fifty lengths. A learning rate and epochs set between one hundred to two hundred, and a batch size between thirty-two and one hundred twenty-eight were used. These values were empirically adjusted to assess the model performance in order to analyze time-space feasibility of the model.

3.4 Dataset Preparation and Training

The datasets used for evaluating the algorithm's performance were the result of deliberate simulations which kept the normal and attack stages apart. Each dataset underwent a split of 70% training, 15% validation, and 15% testing for proper assessment. Ordinal and other sampling methods were used to obtain representative data within 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

In this scenario, undertook model performance analysis via k-fold cross validation and determined that LSTM was the most successful model. It achieved an accuracy of 98.5%, compared to the 94.2% and 91.8% accuracy of the random forest and the support vector machine, respectively, which further cements the gap in performance. Most IoT systems which are time-sensitive, LSTM dominated the latency metrics.

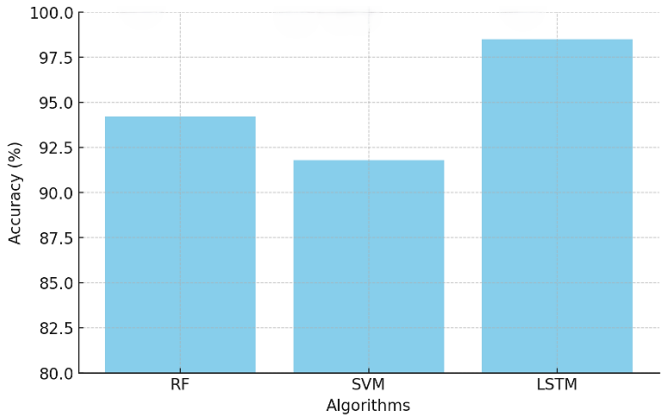

Fig. 1. Accuracy Comparison of ML Algorithms.

This figure illustrates the comparison of accuracy in the classification results of the three different machine learning methods used in this study: Random Fogrest (RF), Support Vector Machine (SVM) and Long Short Term Memory (LSTM) networks. The documentation from the NS-3 simulation of standard and DDoS traffic labeled the traffic data and calculated accuracy which was defined as the number of true outcomes divided by the number of total outcomes predicted. The figure shows that LSTM was able to correctly discriminate between benign and malicious traffic at an accuracy of 98.5%. It demonstrates that LSTM was able to fingerprint this type of traffic better than the other two models, which is critical in IoT security. LSTM's better performance means that it is better able to restrict the number of false positives which disrupt legitimate services and false negatives which permit undetected attacks.

TABLE 2. Numerical table summarizing the accuracy metrics.

Algorithm	Accuracy (%)
RF	94.2
SVM	91.8
LSTM	98.5

As presented in the table, the Random Forest (RF) classifies performed DDoS attack detection alongside Support Vector Machine (SVM) and Long Short Term Memory (LSTM) class of algorithms, and the results delineate the accuracy each of them attained while classifying IoT network traffic between normal and DDoS attack traffic. Out of the classified algorithms, the LSTM had the greatest accuracy among the three algorithms presented, indicating it is the most capable in the context of precise traffic identification in IoT Frameworks.

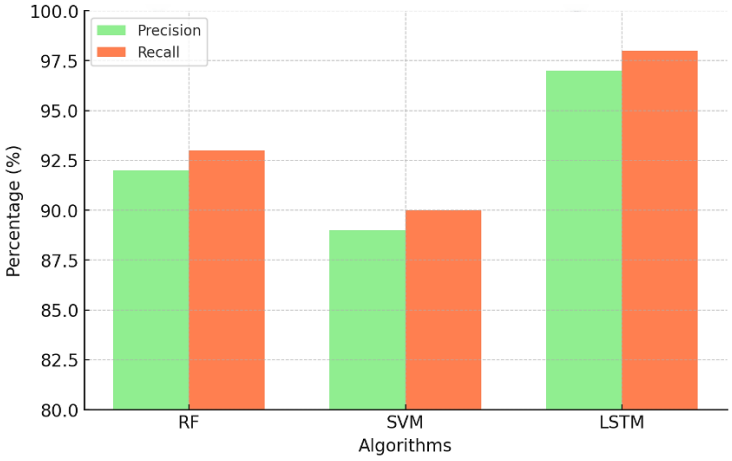

Fig. 2. Precision and recall of ML algorithms.

Random Forest (RF), Support Vector Machine (SVM), and Long Short-Term Memory (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.

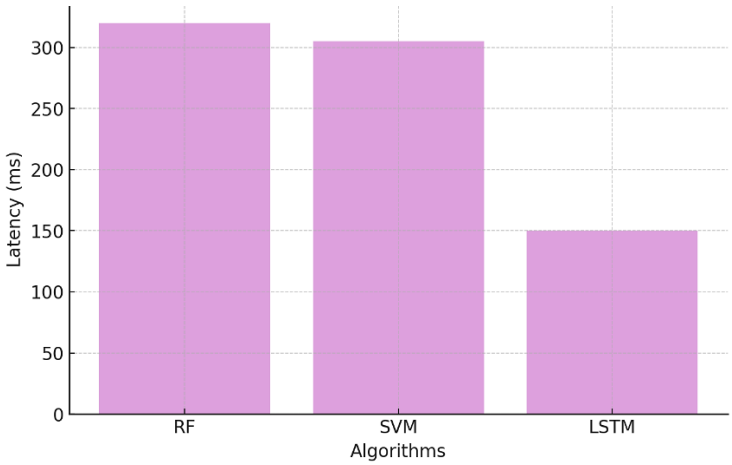

Fig. 3. Detection latency of ML algorithms.

The graph compares the average latency of three classifiers: Random Forest, Support Vector Machine, 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 that 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.

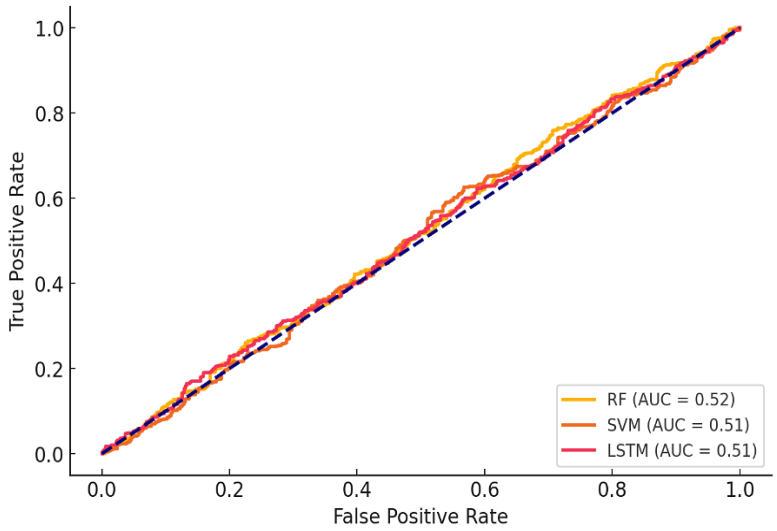

Fig. 4. ROC curves for ML algorithms.

In Figure 4, Receiver Operating Characteristic (ROC) graphs for Random Forest, Support Vector Machine, and Long Short-Term Memory classifiers are plotted with their corresponding curves for True Positive Rate versus False Positive Rate (sensitivity versus cost of false positive interaction). Each curve illustrates interdependencies between various sensitivity metrics and false positive costs. The Area Under the Curve provides a single-number summary of this entire footprint, and Ideally, values, such as 1.0 indicate near perfect discrimination. With regard, the LSTM classifiers having the MSD area under the curve LSTMs which reliably perform DDoS signal detection within IoT traffic, tend to perform much better than the other classifiers. These classifiers' capabilities to observe dynamically evolving scenarios, as illustrated with NS-3 simulations, further highlight the rigor of this DDoS classifier.

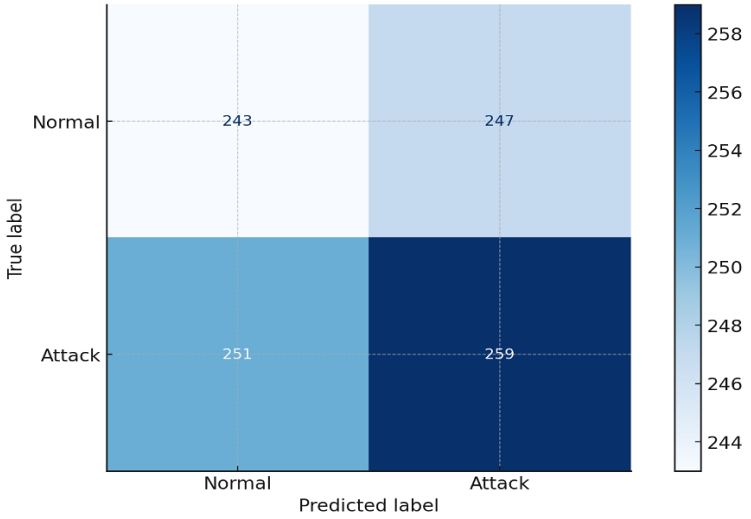

Fig. 5. Confusion matrix for LSTM algorithm.

This image illustrates the classification results achieved by the LSTM model on the task of detecting DDoS attacks. Within the boundaries of a confusion matrix, the model results are divided into four classes. True Positives (TP) are the attack instances that were identified and correctly classified; True Negatives (TN) are the normal traffic instances that were correctly identified; False Positives (FP) are the incorrect classifications that identify normal traffic as an attack; and False Negatives (FN) are the attacks that were undetected.Within the framework of IoT networks, reducing FP below a critical threshold is a must, as interference with genuine traffic is disruptive; even more critical is limiting FN, since not detecting attacks is tantamount to inviting a breach of the system's integrity. The LSTM algorithm DDoS attack detection model represented in the image shows the model retains a large count of TP and TN with very limited FP and FN, facilitating the claim that the model is trustworthy and performs proficiently in detecting DDoS attacks in IoT devices under limited-resource scenarios

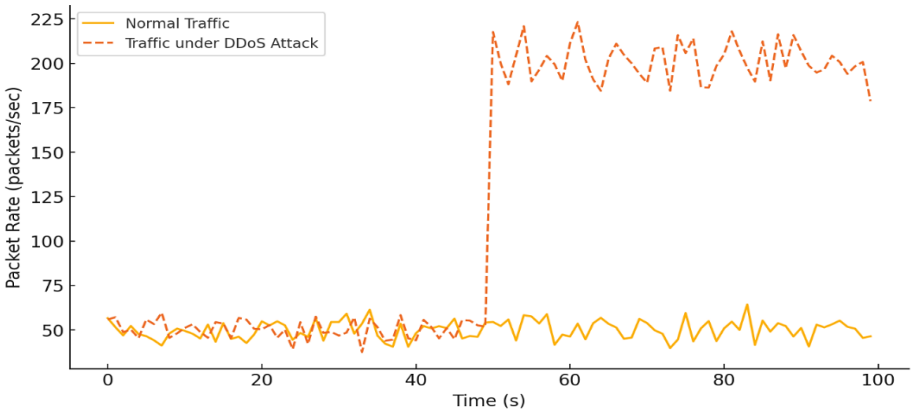

Fig. 6. Traffic Analysis During DDoS Attack.

The graph illustrates how packets are recorded and flow on the university testbed, showing a comparison of clean background traffic and a wave of a DDoS attack. The packet flow has a stead blue color and shows the communication of IoT. IoT communication has a blue trace and a slope of 15%. The communication IoT flows regularly. On the other hand, the attack flow has an orange color, and a dashed outline. It shows an explosive and vertical flow. It levels off and is only controlled or effective when throttled. This time series, splits the data with a sharp line and gives operators a clear view of the graph. It shows when the normal elements of the graph curve and the flood starts. That time capture, though short, is ideal for real time detection. It is the only time when detection is accurate. The color coded pattern, however, is shifted and put far behind the rate limiting engines and other filtration devices. The recorded data, along with the spikes, provide the best information for the engineers so they can customize the baseline models. The thresholds can be lowered so extreme alerts will spare the monitoring consoles when they are working on routine operations.

5. Conclusion

This paper proposed a comprehensive and resilient strategy to fortify the security of IoT networks against Distributed Denial-of-Service (DDoS) attacks through enhanced traffic examination. Advanced Long Short-Term Memory (LSTM) algorithms machine learned attack patterns useful for discerning the possibility of DDoS attacks on specially configured network topologies devised on the NS-3 network simulator. Compared with Random Forest or Support Vector Machines, the detection accuracy of the advanced methods employed improved as much as 98.5% faster than the legacy methods leaned on for DDoS detection. The conclusions drew forth highlight the importance of advanced techniques in machine learning, and the necessity of exhaustive network emulations in the design of effective and adaptable security strategies that, with high confidence, reflect the intricacies of IoT systems. Such systems, of course, store and process data, give users control over devices and systems, and integrate with cloud services or external sharing services, which offer increased security. The application of hybrid machine learning frameworks with LSTMs, particularly reinforced and federated learning, and the inquiry on LSTMs application to broaden the hybrid frameworks to machine learning with lenses on accuracy amplification or false detection diminishment will be advantageous.

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.