جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Enhancing IoT Security in 5G Networks: Mitigating DDoS Attacks With Deep Learning

Reem Alzhrani*, Mohammed Alliheedi
Faculty of Computing and Information, Al-Baha University, Saudi Arabia

Received 11 Oct. 2024; Accepted 08 Dec. 2024; Available Online 31 Dec. 2024

Abstract

The development and implementation of Internet of Things (IoT) devices have accelerated dramatically in recent years. As a result, a robust network infrastructure is required to handle the massive volumes of data collected and transmitted to these devices. Fifth-generation (5G) is a new, comprehensive wireless system with the potential to be the primary enabling technology for the IoT. However, the rapid spread of IoT devices presents significant security challenges. Consequently, new and serious security and privacy risks have emerged. Attackers often exploit IoT devices to launch large-scale attacks, such as the Distributed Denial of Service (DDoS) attack. Recent research shows that deep learning methods are effective in identifying and preventing DDoS attacks. In this paper, we applied four deep learning algorithms: Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Feedforward Neural Network (FNN), and Deep Neural Network (DNN). We compared the results of these algorithms with three machine learning methods: Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Stochastic Gradient Descent (SGD). These methods were used to detect DDoS attacks in a dataset specifically designed for IoT devices within 5G networks. We constructed the 5G network infrastructure using OMNeT++ with the INET and Simu5G frameworks. The dataset encompasses both normal network traffic and DDoS attacks. CNN, FNN, SVM, SGD, and KNN achieved high accuracy, with results reaching up to 99%. In contrast, LSTM and DNN showed significantly lower accuracy. These results demonstrate that deep and machine learning can improve the protection of IoT devices in 5G networks.

I. Introduction

The Internet of Things (IoT) has transformed our lives, including social interactions, communication methods, entertainment, and business practices. As one of the enabling technologies for 5G, IoT supports the coexistence of various technologies. Key requirements for IoT-based 5G networks include high data rates, low latency, and efficient spectrum utilization [1][2]. IoT applications span various fields, such as smart homes, e-health, smart cities, and connected devices [3]. By 2025, the number of IoT devices is expected to surpass 30 billion [4]. Consequently, IoT requires a robust network infrastructure to manage and govern massive data volumes.

Keywords: 5G network, cybersecurity, deep learning, DDoS attack, IoT, machine learning, OMNeT++.

Production and hosting by NAUSS

* Corresponding Author: Reem Alzhrani
Email: rrmsh.92@gmail.com

doi: 10.26735/MVMP8068

5G technology emerges as a comprehensive wireless solution, offering significant benefits like greater network capacity, low latency, high reliability, better spectral efficiency, and increased bandwidth compared to previous generations [5]. However, the growing adoption of IoT devices raises security concerns as attackers exploit vulnerabilities in these devices [3][6]. Common attacks targeting IoT devices include Distributed Denial of Service (DDoS), Denial of Service (DoS), data leakage, malicious code injection, routing attacks, and data transit attacks [7].

A report from Cloudflare highlights a notable increase in DDoS attacks, which were four times higher in Q4 2021 compared to Q3 2021. These attacks pose severe threats to IoT devices, leading to service disruptions, financial losses, and other harmful consequences. It is vital to prepare for DDoS attacks and mitigate their effects proactively. The importance of IoT security is underscored by the potentially devastating consequences of an IoT attack, which can surpass those of a typical web attack that temporarily disrupts user access.

In recent years, Machine Learning (ML) and Deep Learning (DL) have proven effective in detecting and managing DDoS attacks [8]. In this paper, we propose using Deep Learning techniques, specifically Convolutional Neural Networks (CNN) and Feedforward Neural Networks (FNN), to effectively detect and mitigate DDoS attacks on IoT devices within 5G networks. We provide a detailed description of the dataset, network infrastructure, and Deep Learning algorithms employed for DDoS detection. The paper concludes with a discussion of results and future research potential in this area.

The contributions of this paper include.

- Utilizing the OMNeT++ simulation tool with the Simu5G framework to generate a dataset for 5G networks involving IoT devices.
- Applying various Deep and Machine Learning algorithms, such as CNN and Support Vector Machine (SVM), to compare their performance using a specially curated dataset for 5G networks that includes DDoS attacks and normal data traffic.
- Evaluating model performance through a confusion matrix.

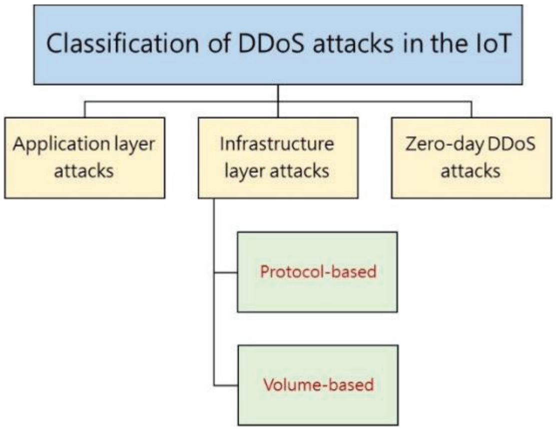
Classification of DDoS attacks in the IoT
Application layer attacks
Infrastructure layer attacks
Zero-day DDoS attacks
Protocol-based
Volume-based

Fig. 1 Classification of DDoS attacks in the IoT [9]

The rest of the paper is structured as follows: Section II discusses DDoS attacks in IoT. Section III discusses Deep Learning. Section IV explores the related work on the effectiveness of using Machine Learning and Deep Learning techniques to detect DDoS attacks. In Section V, we introduce the 5G network, present a novel 5G dataset, and apply Deep Learning models. Section VI presents the results. Finally, Section VII provides the conclusion of the paper, including the highlights of the discussion and areas for further work.

II. Ddos Attacks in IoT

The kind of attack employed in IoT-specific DDoS is not different from general DDoS, where weaknesses are exploited to flood systems. However, the wide range of IoT devices in existence leads to greater diversity and complexity in these types of attacks [9]. These attacks can target not only servers but also network resources, processing units, and storage [10]. As shown in Fig. 1, it is possible to categorize these attacks into three groups according to the tactics used by the attackers [9].

1. Application layer attacks refer to an effort to compromise the application layer of the network architecture. This can occur when packets are dropped as a result of overwhelming the application or web server with a flood of HTTP (Get/Post) requests and other requests that target system software such as Windows, Apache, OpenBSD, and others [9].

2. Infrastructure layer attacks in IoT aim to disrupt systems by exploiting network weaknesses, with two main types: protocol-based and volume-based. Various tactics are used, which include reflection, amplification, and manipulating IP addresses to cause network congestion. Protocol-based attacks, like SYN floods, deplete server resources. While volume-based attacks include UDP/TCP floods and overflow system bandwidth. These tactics result in significant bandwidth wastage [9].
3. Zero-day DDoS attacks can be defined as a new type of emerging DDoS attack that exploits new unknown vulnerabilities in the systems. This kind of attack has recently been a preferred choice of cyber attackers [9].

III. Deep Learning

Neural networks are an advanced subcategory of Machine Learning, commonly referred to as Deep Learning, used for data analysis. It generalizes patterns in a manner similar to the human brain, allowing it to discover trends and make predictions. Deep Learning models, when applied to large and diverse datasets, improve classification accuracy or reduce errors in the used models. Deep Learning is composed of a multilayered neural network, potentially containing thousands of neuronal units between the input and output layers. These intermediate layers, called hidden layers, consist of individual nodes known as "hidden nodes" [11]. Deep Learning represents a wide array of architectures and techniques aimed at achieving specific goals. Below is a brief summary of commonly used models:

1. CNN: A convolutional neural network (CNN) is a deep neural network widely applied in image processing tasks, such as optical character recognition (OCR) and character identification like postal codes. CNNs utilize learnable filters that slide across the input data, generating feature maps. Fully connected layers then operate on these extracted maps to produce the output [12].
2. FNN: A feedforward neural network (FNN) is a straightforward type of artificial neural network, typically comprising three layers: input, hidden, and output. It is particularly effective in pattern recognition and various statistical applications [13].
3. Recurrent Neural Network (RNN): A recurrent neural network (RNN) processes real-time information by leveraging past input memory. Instead of completely forwarding prior data, it incorporates it through links in the network, enhancing its capability via backpropagation, often termed "backpropagation through time" (BPTT) [12].
4. DNN: A deep neural network (DNN) employs multiple layers to make higher-level inferences. These models are built on two-dimensional logistic regression, consisting of input, output, and hidden layers. The term "deep" reflects the inclusion of multiple hidden layers [14].
5. LSTM: A long short-term memory (LSTM) network is a specialized type of RNN that uses a cell structure to retain information over time. This cell structure comprises three gates controlling data flow to decide what to retain or discard. LSTM, developed by Hochreiter and Schmidhuber, is applied in various fields [14][15].

Machine Learning includes numerous architectures and techniques to achieve its objectives. Below is a summary of some commonly used models:

1. SVM: A support vector machine (SVM) is a kernel-based Machine Learning model designed for classification and regression tasks. It maximizes the margin between classes in the training set, enhancing its ability to generalize. SVM is often favored for its strong performance in supervised learning [16].
2. SGD: Stochastic gradient descent (SGD) is an optimization method that reduces computational costs in high-dimensional spaces by introducing randomization. While it converges more slowly, it allows for quicker iterations [17].

3. KNN: The k-nearest neighbor (KNN) algorithm is a simple yet effective technique that assigns labels to unlabeled instances based on their similarity to the dataset's training examples [18].

IV. Related Work

Machine Learning and Deep Learning have proven successful in detecting DDoS attacks on IoT devices. Numerous researchers in this field have conducted experiments and developed innovative approaches. Ma et al. [19] proposed a novel CNN model for detecting DDoS attacks on IoT devices, achieving an accuracy of 92%, outperforming the classical CNN, which achieved 89%. Hussain et al. [20] introduced a new method for detecting DoS and DDoS attacks by converting network traffic data into visual formats. Their approach achieved an impressive 99.99% accuracy in binary classification tests and an average precision of 87% for identifying eleven different attack patterns using a CNN-based architecture (ResNet) on the transformed dataset. This represented a 9% improvement over existing methods, demonstrating the efficiency of CNNs in network security and the importance of data transformation techniques to enhance model performance.

Amaizu et al. [21] developed a DDoS detection framework tailored for 5G and beyond networks, leveraging DNN to enhance detection efficacy. The framework was benchmarked against other models, including SVM, KNN, and CNN, and successfully identified various types of DDoS attacks. Using the CICDDOS2019 dataset, the framework achieved a detection accuracy of 99.66% with minimal loss of 0.011, effectively addressing the DDoS problem.

Alnuman et al. [22] simulated an IoT home network, including a DDoS attack, using OMNeT++. They generated traffic with and without injected attacks to test the accuracy of Machine Learning methods for DDoS detection. Analysis using Decision Forest, Decision Jungle, and a Boosted Decision Tree revealed accuracy rates of 83.80%, 83.20%, and 99.90%, respectively. Al-Qahtani [23] proposed a hybrid optimized LSTM approach to predict various network attacks, including DoS, DDoS, man-in-the-middle, and spoofing. This approach combined CNN for feature extraction with LSTM for prediction. Data was collected using OMNeT++ and other datasets like CIDCC-15, UNSW-NB15, and NSL-KDD, showcasing the effectiveness of Deep Learning-based intrusion detection systems.

TABLE I
Related Work

Reference	Advantages and Disadvantages
Ma et al [19]	Pros: The novel CNN model has proven highly effective in detecting DDoS attacks on IoT devices. Cons: The study has not been applied to 5G networks in IoT devices.
Hussain et al. [20]	Pros: The study proposed transforming network traffic into image representations for analysis using the ResNet CNN model, achieving high accuracy and demonstrating its effectiveness in detecting DoS and DDoS attacks. Cons: The study has not been applied to 5G networks in IoT devices.
Amaizu et al. [21]	Pros: This study has proven the effectiveness of DNN in DDoS attacks on the CICDDOS2019 dataset for 5G and beyond 5G networks. Cons: No simulator was employed to simulate real 5G networks on IoT devices. Instead, a pre-collected dataset containing DDoS attacks was used.
Alnuman et al. [22]	Pros: Various Machine Learning algorithms have been employed successfully in DDoS attacks in IoT networks. An OMNeT++ simulator was used to create the IoT network. Cons: Deep Learning algorithms have not been applied, and their effectiveness has not been applied to 5G networks in IoT devices.
Al-Qahtani [23]	Pros: The study proposed a novel hybrid optimized LSTM approach to predict various network attacks, including DDoS. A CNN was implemented to extract features from the IoT network, improving the accuracy of attack detection. Data was collected using OMNeT++, and additional datasets were employed to evaluate the performance of different Deep Learning-based intrusion detection systems. Cons: The study has not been applied to 5G networks in IoT devices.
Bishnoi et al. [24]	Pros: The study presents a new Deep Learning method for real-time DDoS detection in IoT fog environments, combining CNN and LSTM networks with high accuracy and a low false alarm rate. Cons: The study has not been applied to 5G networks in IoT devices.

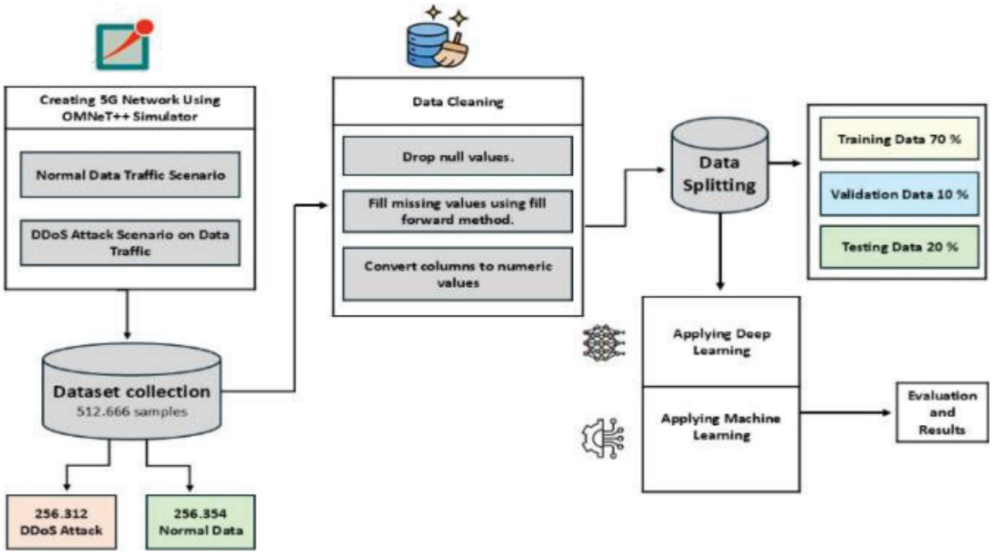

Fig. 2 Proposed Methodology

Bishnoi et al. [24] presented a novel Deep Learning methodology for detecting DDoS attacks in fog environments involving IoT devices. Their approach combined CNN and LSTM networks to monitor network traffic and identify DDoS attacks in real-time. Experimental results highlighted the effectiveness of this method, achieving high detection accuracy with a low false alarm rate.

Materials and Methods

In this section, we outline the 5G network utilized in this study, detailing the process of dataset extraction and the application of Deep Learning techniques for its analysis. Fig. 2 provides an overview of the proposed methodology

A. 5G Network

To establish our 5G network, we chose OMNeT++ for several reasons. It has a friendly graphical user interface (GUI) that makes the conduct of simulations easy. Furthermore, OMNeT++ is an open-source tool [25]. OMNeT++ integrates the Simu5G framework in order to enhance the effectiveness of creating 5G networks [26]. We installed OMNeT++ on an Ubuntu operating system, effectively integrating it with both the Simu5G and INET frameworks. Moreover, we utilized the NED programming language, and the respective versions of these components are presented in Table II.

TABLE II
Experiment Tools for 5G Topology

No	Tool	Version
1	Ubuntu OS	20.4
2	OMNeT++	6.0.1
3	Simu5G	1.2.1
4	INET	4.5

1. Ubuntu: An open-source and free operating system, Ubuntu is built upon the Linux kernel and meant for deployment on personal computers, electronic devices, and servers [27].
2. OMNeT++: Is a powerful and flexible simulation library and framework created using C++, tailored specifically for building network simulators [28].
3. Simu5G: Is an innovative simulation tool that models the data plane of 5G RAN and core networks and is the product of a partnership between Intel Corporation and the Computer Networking Group at the University of Pisa, Italy. This tool is constructed with the OMNeT++ and INET frameworks and is specifically designed for simulating 5G New Radio and LTE networks [29].
4. INET Framework: Is an open-source OMNeT++ library of models for simulating

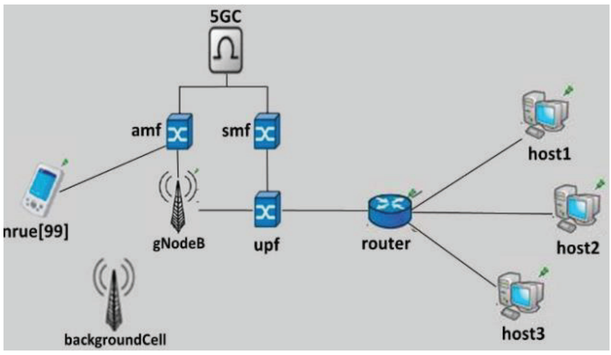

Fig. 3. Architecture of our 5G network [35].

communication networks. It encompasses Internet protocols and link layer protocols (wired and wireless) and provides the base for other simulation frameworks. It's a useful tool for researchers and students working on communication networks, as it allows them to design and test new protocols and explore different scenarios [30].

5. NED: Is the topology description language of the OMNeT++ simulation environment, with the help of which the structure of a simulation model is described. It allows the user to declare simple modules, compound modules, and network definitions, specifying the modules' interfaces with gates and parameters and defining the submodules and their connections. The NED language has been designed to extend the applicability of the OMNeT++ simulation models due to the complexity and growing size [31].

This study meticulously outlines the network architecture of our 5G network, as depicted in Fig. 3. This architecture comprises critical network elements, encompassing a gNodeB (gNB), backgroundCell, router, 100 New Radio User Equipment (NRUe) devices considered IoT devices, three hosts, and integral components of the 5G Core (5GC).

1. gNB: A 5G network node that manages resource management, mobility, and radio communication between user equipment (UE) and the core network [32].
2. backgroundCell: Is a supporting or additional cell that offers more capacity and coverage.
3. 5GC: The 5GC consists of several essential subcomponents required for enabling message transmission and authentication between devices. In Fig. 3, we included several of these subcomponents.
   - Access and Mobility Management (AMF): Handles signaling communication between the UE and the Core Network. It also manages authentication and security protocols, as well as procedures for when the UE is in idle mode [33].
   - User Plane Function (UPF): Acts as a gateway that connects the Radio Access Network (RAN) to the Internet. It is responsible for directing and transmitting data packets [33].
   - Session Management Function (SMF): Is responsible for managing sessions and assigning IP addresses to UE. It is also responsible for choosing and staffing the UPF for data transmission [34].

During the configuration process of the network, we dispersed the locations of individual nodes throughout the network topology.

B. Details of the simulation:

- **Ipv4NetworkConfigurator:** We configured it to enable the dumping of various network configuration details during the simulation. These details included the IP addresses assigned to each network interface in the topology, network topology information such as which nodes were connected to which others, bandwidth and delay information, and routing information such as which paths traffic took between nodes. By enabling these settings, the simulation was able to output detailed information about the network configuration and behavior, which could be utilized to debug issues or analyze the simulation results.
- **Routing settings:** We configure the routing settings by assigning the Global Address Resolution Protocol (ARP) to all nodes with an IPv4 module and how packets are routed between nodes.
- **Visualization settings:** The purpose of the visualization settings is to display the IP addresses on the simulation image.

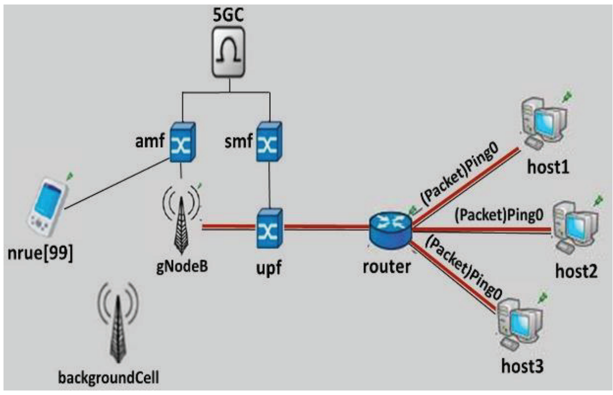

Fig. 4. Second scenario DDoS attack [35].

- General Physical Layer parameters: We added the parameters required for configuring the NRUe devices and the gNB.

C. Network Scenarios

Our network operates in two distinct scenarios: the first is during normal data traffic, and the second is a DDoS attack.

- First scenario Normal data traffic: As shown in Fig. 3, our network operates similarly to others, allowing the normal flow of data traffic between devices. All devices connected to the 5G network can communicate with each other by sending PING, ensuring that data traffic reaches its intended destination.
- Second scenario DDoS attack: In this scenario, we have introduced three host devices that are directly connected to the router, as depicted in Fig. 4. In this case, our goal is to create a DDoS traffic stream to attempt to sever communication between each node. We achieve this by generating packets of unusually large size (1000 bytes) from all hosts and transmitting them at an exceptionally high speed (0.001 seconds) continuously. It is worth noting that this packet size is considerably larger than the largest packet size that a host is typically required to accept, which is only 576 bytes [36]. The DDoS attack is transmitted to all units on the network, and a disrupted communication pattern is seen as abnormal traffic. Instead, communication is lost when the devices cannot communicate with each other.

TABLE III
Features in our 5G Network Dataset

No	Features	No	Features
1	sumweights	9	mean
2	type	10	stddev
3	module	11	min
4	name	12	max
5	attrname	13	underflows
6	attrvalue	14	overflows
7	value	15	binedges
8	count	16	binvalues

D. Creating a Dataset with our 5G Networks

We compiled a dataset that consists of 512,666 samples, including both benign data and DDoS attacks, with 16 features shown in the following Table III. The count of benign samples reached 256,354, while the count of DDoS attacks amounted to 256,312.

E. Preprocessing

In our dataset, we have a large amount of null values, and we need to remove them. We will remove the columns with the least amount of data, specifically `count', `sumweights', `mean', `stddev', `min', `max', `underflows', `overflows', `binedges', and `binvalues'. We are filling missing values using the forward-fill method and converting columns to numeric values.

F. Applying Deep and Machine Learning

This section will discuss the Deep and Machine Learning algorithms that were used in this research for detecting DDoS attacks in 5G networks for IoT devices. For Deep Learning CNNs, LSTMs, FNNs, and DNNs were used, and we compared the results with three Machine Learning algorithms: SVM, KNN, and SGD.

V. Result and Discussion

To evaluate the performance effectiveness of our models in detecting DDoS attacks within our 5G dataset, we utilize the confusion matrix, and a variety of measures derived from established equations. These are very useful performance measurements during model assessment.

1. **Accuracy:** Calculating the accuracy rate for the entire model is according to the following equation:

$$\frac{TP + TN}{TP + TN + FP + FN} \qquad 14$$

2. **Recall:** Calculating the detection rate for the entire model is according to the following equation:

$$\frac{TP}{TP + FN} \qquad 14$$

3. **Precision:** Shows the accuracy of correct positive predictions according to the following equation:

$$\frac{TP}{TP + FP} \qquad 37$$

whereas:

TP = True Positives.

TN = True Negatives.

FP = False Positives.

FN = False Negatives.

The dataset is divided into two subsets: 80% for training and validation, and 20% for testing. Within the training and validation set, 70% is allocated to training data and 10% to validation data. This results in 410,132.8 training samples and 102,533.2 testing samples. It is important to note that the features in our dataset have varying value ranges. To ensure that larger values do not dominate smaller ones, we employ the Min-Max Scaler. This scaling technique uses linear normalization to map all feature values onto a (0,1) scale. The results of the models are summarized in Table V.

Based on the results obtained, it was found that the KNN algorithm achieved the highest accuracy at 99.83%, followed by the SVM algorithm with an accuracy of 99.75%, and the CNN algorithm with an accuracy of 99.74%. Next was the FNN algorithm with an accuracy of 99.53%, and finally, the SGD algorithm with an accuracy of 99.27%. However, two algorithms achieve significantly poorly compared to the previously mentioned algorithms. That is, the DNN algorithm achieved an accuracy of 50%, while the LSTM algorithm achieved an accuracy of 49%, while they both demonstrated 64.73% in F1 score.

TABLE V
Result of applying Deep and Machine Learning models to our 5G network dataset

Model	Accuracy	Precision	Recall	F1 Score
CNN	99.74%	99.87%	99.61%	99.74%
LSTM	49.99%	62.97%	%80.60	%64.73
FNN	99.53%	99.53%	99.54%	99.53%
DNN	50.14%	55.97%	%80.61	64.74%
SVM	99.75%	99.88%	99.62%	99.75%
KNN	99.83%	99.81%	99,84%	99.83%
SGD	99.27%	98,59%	99.97%	99.27%

The KNN algorithm delivered the best prediction results for detecting DDoS attacks in our dataset and is recognized as one of the top 10 algorithms in data mining [38]. KNN demonstrated exceptional effectiveness after determining the optimal value of kkk, which was found to be 5 for our dataset.

The SVM algorithm also showed high performance in both binary and multi-class classification, particularly when applied to challenging datasets that are large, imbalanced, or contain low-quality data [39]. Data classification was performed using the radial basis function (RBF) kernel, with five-fold cross-validation employed to ensure robust evaluation.

CNN proved significantly effective, utilizing multiple 1D convolutional layers and 1D MaxPooling layers. The preference for 1D convolutional layers over 2D layers was driven by their faster training time and the lack of a requirement for a dedicated GPU [40].

The FNN architecture, consisting of multiple hidden and fully connected layers, exhibited strong predictive capabilities. This structure effectively differentiated between normal traffic and DDoS attacks within the dataset.

The SGD classifier performed well in binary classification tasks, with three-fold cross-validation used for evaluation. While its precision reached 98%, it was the lowest among the tested models, as other models achieved a precision of 99%.

As mentioned earlier, the DNN and LSTM models achieved lower accuracy compared to the other models. However, this does not imply ineffectiveness in detecting DDoS attacks or binary classification tasks. Rather, it suggests that these models may not be fully compatible with our dataset. Performance variations could result from factors such as model architecture and the characteristics of the training data. Further experimentation, including hyperparameter tuning and alternative preprocessing techniques, may enhance the performance of these models in future studies.

The DNN model employed a simple architecture, inspired by the remarkable results achieved by other Deep Learning models despite their simplicity

In this study, each model demonstrated distinct advantages and limitations. The CNN model achieved remarkable results, effectively extracting relevant features from data and handling noise and irrelevant information, although it required significant computational resources for training. The LSTM model, well-suited for time-series and sequence-based tasks, produced the lowest results and also demanded considerable computational power.

The FNN model delivered excellent performance, was straightforward to implement, and had fast training times; however, it required more memory. The DNN model, despite its complexity, did not achieve satisfactory results and consumed significant computational resources. The SVM model performed exceptionally well but was sensitive to kernel selection and hyperparameters, requiring substantial resources during training.

The KNN model, though simple and easy to use, produced strong results but also required considerable computational power. The SGD model demonstrated good performance, was memory-efficient, and had relatively low computational demands, but it required careful parameter tuning.

Overall, each model showcased unique strengths and weaknesses, and their suitability depends on the specific requirements and constraints of the task.

VI. Conclusion

In this paper, we applied four Deep Learning algorithms—CNN, LSTM, FNN, and DNN—and compared the results with three Machine Learning algorithms—SVM, KNN, and SGD—to detect DDoS attacks in a dataset specifically designed for IoT devices within 5G networks. The performance of our models was evaluated using a confusion matrix. CNN, FNN, SVM, SGD, and KNN achieved high accuracy levels of 99%, whereas LSTM and DNN recorded accuracy levels of 49% and 50%, respectively. These results demonstrate that Deep and Machine Learning algorithms can significantly enhance the protection of IoT devices in 5G networks.

For future work, we propose experimenting with alternative models beyond those used in this study. Additionally, we recommend utilizing the NETA framework within OMNeT++, which facilitates the generation of various attacks and their detection using the integrated TensorFlow framework. Furthermore, creating complex scenarios with OMNeT++ frameworks, such as simulating a group of drones covering different locations, could add value. These drones, which can be moved using X-Plane software, may simulate potential DDoS attacks. We suggest leveraging the TensorFlow framework embedded in OMNeT++ to efficiently detect and mitigate these attacks.

Acknowledgment

Words could not express our gratitude to Dr. Abdullah Alomari and Dr. Najib Ben Aoun, graciously shared their knowledge and provided invaluable feedback that enabled us to refine this study.

Conflict of Interest

Authors declare that they have no conflict of interest.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16-32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[2] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, "IoT Connectivity Technologies and Applications: A Survey," *IEEE Access*, vol. 8, pp. 67646-67673, 2020, doi: 10.1109/ACCESS.2020.2985932.

[3] S. I. Al-Sharekh and K. H. A. Al-Shqeerat, "An Overview of Privacy Issues in IoT Environments," *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*, Al Madinah Al Munawwarah, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/AECT47998.2020.9194197.

[4] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, Jun. 2020, doi: 10.3390/app10124102.

[5] M. Pons, E. Valenzuela, B. Rodríguez, J. A. Nolazco-Flores, and C. Del-Valle-Soto, "Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties—A Review," Sensors, vol. 23, no. 8, p. 3876, 2023, doi: 10.3390/s23083876.

[6] A. Kumari, D. Gupta, and M. Uppal, "Unifying RNN and KNN for Enhancing Mirai Attack Detection in IoT Networks," *2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, Bangalore, India, 2024, pp. 1-5, doi: 10.1109/ICITEICS61368.2024.10625616.

[7] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. Alsulaimy, "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," *IEEE Access*, vol. 12, pp. 57128-57149, 2024, doi: 10.1109/ACCESS.2024.3382709.

[8] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon, and D. Siracusa, "Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 876–889, Jun. 2020, doi: 10.1109/tnsm.2020.2971776.

[9] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, Jul. 2019, doi: 10.1007/s11235-019-00599-z.

[10] K. Kaur and J. Ayoade, "Analysis of DDoS Attacks on IoT Architecture," *2023 10th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Palembang, Indonesia, 2023, pp. 332-337, doi: 10.1109/EECSI59885.2023.10295766.

[11] S. Dong, P. Wang, and K. Abbas, "A survey on Deep Learning and its applications," *Computer Science Review*, vol. 40, p. 100379, May 2021, doi: 10.1016/j.cosrev.2021.100379.

[12] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A Survey of Deep Learning and Its Applications: A New Paradigm to Machine Learning," *Archives of Computational Methods in Engineering*, vol. 27, Jun. 2019, doi: 10.1007/s11831-019-09344-w.

[13] W. Zhang, H. Li, Y. Li, H. Liu, Y. Chen, and X. Ding, "Application of Deep Learning algorithms in geotechnical engineering: a short critical review," *Artificial Intelligence Review*, vol. 54, no. 8, pp. 5633–5673, Feb. 2021, doi: 10.1007/s10462-021-09967-1.

[14] T. Khempetch and P. Wuttidittachotti, "DDoS attack detection using deep learning," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 2, p. 382, Jun. 2021, doi: 10.11591/ijai.v10.i2.pp382-388.

[15] A. Sherstinsky, "Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network," *Physica D: Nonlinear Phenomena*, vol. 404, p. 132306, Mar. 2020, doi: 10.1016/j.physd.2019.132306.

[16] J. Cervantes, F. Garcia-Lamont, L. Rodríguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: Applications, challenges and trends," *Neurocomputing*, vol. 408, no. 1, pp. 189–215, Sep. 2020, doi: 10.1016/j.neucom.2019.10.118.

[17] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science*, vol. 2, no. 3, pp. 1–21, Mar. 2021, doi: 10.1007/s42979-021-00592-x.

[18] S. Messaoud, A. Bradai, S. H. R. Bukhari, P. T. A. Quang, O. B. Ahmed, and M. Atri, "A survey on machine learning in *Internet of Things*: Algorithms, strategies, and applications," Internet of Things, vol. 12, p. 100314, Dec. 2020, doi: 10.1016/j.iot.2020.100314.

[19] L. Ma, Y. Chai, L. Cui, D. Ma, Y. Fu, and A. Xiao, "A Deep Learning-Based DDoS Detection Framework for Internet of Things," *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148944.

[20] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," *2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 2020,

pp. 1-6, doi: 10.1109/INMIC50486.2020.9318216.

[21] G. C. Amaizu et al., "Composite and Efficient DDoS Attack Detection Framework for B5G Networks," *Computer Networks*, vol. 188, p. 107871, Apr. 2021, doi: 10.1016/j.comnet.2021.107871.

[22] I. A. Alnuman and M. Al-Akhras, "Machine Learning DDoS Detection for Generated Internet of Things Dataset (IoT Dat)," *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257714.

[23] A. S. Alqahtani, "FSO-LSTM IDS: Hybrid Optimized and Ensembled Deep-Learning Network-Based Intrusion Detection System for Smart Networks," *The Journal of Supercomputing*, Jan. 2022, doi: 10.1007/s11227-021-04285-3.

[24] S. Bishnoi, S. Mohanty, and B. Sahoo, "A Deep Learning-Based Methodology in Fog Environment for DDoS Attack Detection," *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2021, pp. 201-206, doi: 10.1109/ICCMC51019.2021.9418363.

[25] P. A. B. Bautista, L. F. Urquiza-Aguiar, L. L. Cárdenas, and M. A. Igartua, "Large-Scale Simulations Manager Tool for OMNeT++: Expediting Simulations and Post-Processing Analysis," *IEEE Access*, vol. 8, pp. 159291-159306, 2020, doi: 10.1109/ACCESS.2020.3020745.

[26] G. Nardini, D. Sabella, G. Stea, P. Thakkar, and A. Virdis, "Simu5G–An OMNeT++ Library for End-to-End Performance Evaluation of 5G Networks," *IEEE Access*, vol. 8, pp. 181176-181191, 2020, doi: 10.1109/ACCESS.2020.3028550.

[27] CANONICAL Organization, "Download Ubuntu desktop," [Online]. Available: https://ubuntu.com/download/desktop. [Accessed: Jan. 27, 2023].

[28] OMNeT++ Organization, "OMNeT++," [Online]. Available: https://omnetpp.org/. [Accessed: Jan. 15, 2023].

[29] OMNeT++ Organization, "Simu5G," [Online]. Available: https://omnetpp.org/download-items/simu5g.html. [Accessed: Jan. 15, 2023].

[30] OMNeT++ Organization, "INET Framework," [Online]. Available: https://omnetpp.org/download-items/inet.html. [Accessed: Jan. 15, 2023].

[31] A. Varga and R. Hornig, "An Overview of the OMNeT++ Simulation Environment," *Proceedings of the First International ICST Conference on Simulation Tools and Techniques for Communications Networks and Systems*, 2008, doi: 10.4108/icst.simutools2008.3027.

[32] U. Kingdom, "What is a GNB (gNodeB)?," Inseego.com, [Online]. Available: https://inseego.com/uk/resources/5g-glossary/what-is-gnb/. [Accessed: Nov. 19, 2024].

[33] M. DeNapoli, "Get to Know 5G – Part 1," Cisco Blogs, Nov. 22, 2021. [Online]. Available: https://blogs.cisco.com/developer/gettoknow5g0. [Accessed: Jan. 27, 2023].

[34] P. Salva-Garcia, J. M. Alcaraz-Calero, Q. Wang, J. B. Bernabe, and A. Skarmeta, "5G NB-IoT: Efficient Network Traffic Filtering for Multitenant IoT Cellular Networks," *Security and Communication Networks*, vol. 2018, pp. 1–21, Dec. 2018, doi: 10.1155/2018/9291506.

[35] R. M. Alzhrani and M. Alliheedi, "5G Networks and IoT Devices: Mitigating DDoS Attacks with Deep Learning Techniques," arXiv (Cornell University), Nov. 2023, doi: 10.48550/arxiv.2311.06938.

[36] C. Shannon, D. Moore, and K. C. Claffy, "Beyond Folklore: Observations on Fragmented Traffic," *IEEE/ACM Transactions on Networking*, vol. 10, no. 6, pp. 709-720, Dec. 2002, doi: 10.1109/TNET.2002.805028.

[37] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS Attacks with Feed Forward-Based Deep Neural Network Model," *Expert Systems with Applications*, vol. 169, p. 114520, May 2021, doi: 10.1016/j.eswa.2020.114520.

[38] S. Zhang, "Challenges in KNN Classification," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 10, pp. 1–1, 2021, doi: 10.1109/TKDE.2021.3049250.

[39] W. Dudzik, J. Nalepa, and M. Kawulok, "Evolving Data-Adaptive Support Vector Machines for Binary Classification," *Knowledge-Based Systems*, vol. 227, p. 107221, Sep. 2021, doi: 10.1016/j.knosys.2021.107221.

[40] S. Kiranyaz, O. Avci, O. Abdeljaber, M. Gabbouj, and D. Inman, "1D Convolutional Neural Networks and Applications: A Survey," *Mechanical Systems and Signal Processing*, vol. 151, p. 107398, Apr. 2021, doi: 10.1016/j.ymssp.2020.107398..