

Deep Learning Approaches for DDoS Attack Detection in Communication Networks and IoT: A Comprehensive Review

Nabeel Fouad Abdulrahman^{a*} & Mandeep Singh Jit Singh^b

^aCommunication System Engineering, Baghdad, Iraq

^bDepartment of Electrical, Electronic & Systems Engineering, Faculty of Engineering & Built Environment, Universiti Kebangsaan Malaysia, 43600 UKM Bangi

*Corresponding author: P125278@siswa.ukm.edu.my

Received 27 February 2024, Received in revised form 24 October 2024
 Accepted 24 November 2024, Available online 30 January 2025

ABSTRACT

The increasing adoption of transformative technologies, such as the Internet of Things (IoT), has brought convenience and optimization to various domains. However, it has also introduced new challenges, including the vulnerability to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. DDoS attacks have shown an alarming rise in frequency and potency, making it crucial to devise efficient mechanisms to prevent such attacks and safeguard communication networks. IoT networks, with their numerous interconnected devices and limited resources, are particularly susceptible to DDoS attacks. Traditional rule-based approaches have proven insufficient to cope with the dynamic nature of modern attacks, leading to the emergence of deep learning-based detection and mitigation techniques. Deep learning models, supported by real-world datasets, offer promising results with detection rates exceeding 98%. This study explores various deep learning architectures, focusing on their success in DDoS attack detection, particularly in IoT networks. It also addresses the challenges associated with such networks and highlights potential areas for future research.

Keywords: Convolutional Neural Networks (CNNs); deep learning; Distributed Denial of Service (DDoS); Internet of Things (IoT); Long Short Term Memory (LSTM); transfer learning

INTRODUCTION

The landscape of information and technology is evolving rapidly. Many transformative paradigms like the Internet of Things (IoT) have emerged, that allow devices and objects to communicate autonomously. The recent stats suggest that the estimated number of IoT devices has reached over 42 billion following an exponential rise (statistica, 2023). Such enhancements have brought in convenience and optimized many systems including healthcare, industries, smart homes, etc. (Pradhan et al. 2021; Talavera et al. 2017) Despite such enablement, numerous challenges are associated with such IoT networks. Two such challenges are Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks (Džaferović et al. 2019). Statistics indicated by the global DDoS threat reports suggest that DDoS attacks have increased by more than 115 percent during 2022 (Microsoft

2023). Also, the average attack size suggested is over 500 Gbps according to the reports (Cook 2023). These figures highlight the importance of devising mechanisms that can prevent DDoS attacks, and safeguard the IoT and other communication networks.

IoT networks comprise numerous nodes and connected devices, in the form of sensors, actuators, processing systems, and communication parts (Aleesa et al. 2020). Such devices perform the data communication and processing tasks based on which several actions are derived. One common aspect of such networks is their limited resources in terms of processing and power, thus residing on relatively poor security measures, making them susceptible to various kinds of attacks (Mohanta et al. 2020). Additionally, with the diversity attained in such networks in the form of manufacturing standards and operational standards (broadband IoT, Narrowband IoT, etc.), the development of universal security protocols is

becoming even more challenging (Benkhelifa et al. 2018). Such a massive attack surface comprising thousands of connected devices further exacerbates the associated vulnerabilities. A study conducted by Kaspersky revealed that over 30 percent of IoT devices suffered from attempted attacks during the first two quarters of the year 2022 (Kaspersky, 2022). By exploiting such a large attack surface, attackers are enabled to launch DDoS attacks, that can lead to causing disruptions in the system.

In a typical DDoS attack scenario in IoT networks, attackers attempt to flood the target systems with commands and data traffic, that makes the system incapable of processing the actual information (Kumari & Jain, 2023). This leads to the network getting unbearable congestion and leads to complete disruption of the system. Attackers exploit the compromised nodes and devices to enter into the networks, and make use of botnets (in general), to produce attack data traffic (Vishwakarma & Jain 2020). Some of the traditional approaches developed earlier to mitigate and detect such attacks generally resided on rule-based techniques that were unable to cope with the increasing surface and dynamic nature of such attacks (Rajendran et al. 2019). Additionally, once the attackers invade a network, they can capture other applications and infrastructure of the organizations simultaneously. According to a report by Radware, 86 percent of the organizations suffered from such multi-vector DDoS attacks (Radware 2021). This gave rise to the adoption of some real-time and robust attack detection mechanisms, that can identify malicious traffic and able to kill such attacks are their inception stages.

The development of modern DDoS attack detection and mitigation techniques is, therefore, inevitable considering the consequences that can be brought along with such attacks including financial loss, reputational damage, and even physical harm. To cater to such issues, the use of deep learning in DDoS attack detection has emerged and is today seen as an efficient approach to enhance detection and mitigation capabilities. According to some research published (Dora & Lakshmi 2022; Haider et al. 2020), deep learning is capable of detecting DDoS attacks over 98 percent of the time. Residing on the sophisticated architecture of neural networks, and supported by real-world datasets, deep learning develops the intricate attack patterns and makes the networks block those nodes to prevent further spreading. Additionally, these methods can learn from the dynamics of the attacks as well which makes them stand out from the traditional approaches.

This study focuses on exploring various architectures of deep learning that have been used in the past and has proven to be successful in DDoS attack detection in general and communication networks (especially IoT networks).

Additionally, some of the challenges associated with the use of such networks will be explored and presented as part of future research.

RELATED WORKS

In the domain of cyber security, DDoS attacks have remained one of the greatest challenges due to their dynamic nature. Traditionally, the attack detection mechanisms have been divided into two categories: signature-based and anomaly-based detection (Otoum & Nayak 2021). In the signature-based detection methods, some of the attack patterns are determined. Upon reaching a match with such patterns, a trigger is generated. This technique can be highly accurate in making detections, yet it may fail under the dynamics and evolving nature of the attacks. Anomaly-based detection works by establishing a baseline for the network to operate under normal conditions. Any deviation from such conditions helps in detecting the potential presence of attack traffic. Thus, the method can detect unknown DDoS attacks, yet it also can lead to an increased number of false positives and may render network performance to be less optimal. The research articles published on DDoS attack detection in IoT networks using traditional methods explore numerous techniques and characteristics of IoT networks. Methods like feature engineering (Bonaccorso 2017) have been adopted to distinguish between legitimate and malicious network traffic. The limited resources of IoT devices have also been catered to while presenting the methods for DDoS attack detection and prevention. The dynamics associated with the IoT traffic coupled with the evolving nature of the IoT networks have brought further challenges in curtailing the threat landscape. While these articles and ideas have been discussed as part of ensuing sections, this section focuses on some of the fundamental deep learning concepts that serve as a baseline.

The ability of deep learning is instrumental in learning from the dynamic nature of attack patterns autonomously. At the core of deep learning are numerous architectures of the neural networks including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), etc. (Shrestha & Mahmood 2019) that can learn from the intricate patterns contained inside the data without residing on manual feature extraction. These traits have enabled deep learning to demonstrate an ability to perform exceptionally well in malware attack detection spam filtering, etc.

Numerous surveys have been published on DDoS attack detection and their mitigation techniques. Yet many of them cover the traditional methods of attack detection

and defense mechanisms in a general communication setting. The information related to DDoS attack detection and the network areas prone to such attacks is tremendously available in the literature, which can serve as a baseline for the development of advanced models. In the existing surveys, (Zargar et al. 2013) presented a survey paper where various types of DDoS flooding attacks have been presented. These include the botnet-based DDoS attacks and some of their types. However, the survey remained specific to present the known attack yet it does not incorporate the dynamics of the DDoS landscape. Additionally, the survey covers the broader areas of attack detection and is not specific to IoT networks. (Sonar & Upadhyay, 2014) present a survey that represents security issues in IoT networks in general. DDoS attacks have been presented as part of those security issues where the layered architecture of the IoT networks has been explored and discussed. Yet the paper provides insufficient information on the taxonomy of DDoS attacks, their types, and methods to create a defense mechanism against them. (Zhang & Green, 2015) go one step ahead in presenting the survey, where apart from discussing the security issues in IoT networks, the taxonomy of DDoS attacks and defense mechanisms has been presented. Some of the traditional approaches have been explored that can lead to reduced attacks and less damage caused to the network infrastructure. (Yang et al. 2017) present a broader picture of DDoS attacks presenting the existence of botnets and malware in the DDoS attack arena. The taxonomy of DDoS attacks has been presented in the context of IoT networks while highlighting the security issues in IoT networks in general. (Abdul-Ghani et al. 2018) apart from following a similar review roadmap of presenting the security issues, taxonomy, and malware, also highlighted some of the open challenges. Yet it does not cater to the dynamics and evolving nature of the malware and DDoS attack methods. (Vishwakarma & Jain, 2020) presented a holistic picture of DDoS attack detection and mitigation where various issues have been discussed related to security in IoT networks, and the taxonomy of DDoS attacks. The defense methods covered the traditional and non-traditional approaches where the role of machine learning has been highlighted. Yet, a comprehensive overview of deep learning and its use in DDoS attack detection in IoT networks is found missing.

Some of the review papers target Intrusion Detection Systems (IDS) and DDoS attack detection under machine learning and deep learning as well. (Ferrag et al. 2020) present an overview of IDS methods using deep learning. Some of the other review articles include (Ahmad & Alsmadi, 2021; Ahmad et al. 2021; Aleesa et al. 2020; Gamage & Samarabandu 2020) where IDS security has been discussed under various machine learning and deep learning approaches. (Mittal et al. 2022) takes into consideration DDoS attack detection while making a review of deep learning methods, yet the review extensively focuses on the use of benchmark DDoS datasets, instead of establishing a general and methodology-based segmentation of the deep learning algorithm. The focus therefore remains on the adoption of suitable pre-processing, and specific network architecture.

Our survey focuses on DDoS attack detection under the dynamics attack conditions and incorporates the evolving nature of DDoS attacks specific to the IoT environment. To do this, the types of deep learning methods successfully used for the detection and mitigation of DDoS attacks have been presented. The paper instead of focusing on the existing types of attacks, focuses on a generalized deep-learning approach that can autonomously cater to such an evolving nature. This includes the type of deep learning approaches that can be used including convolutional networks, recurrent networks, etc. In Table 1, a comparison between the existing review articles presented above, and our review articles has been provided. The main contribution of this survey paper is, therefore, as follows:

1. Instead of focusing on the traditional survey methodologies presented before, where security issues in IoT networks are highlighted while presenting the case of DDoS attack taxonomy and some traditional mitigation techniques, this paper caters to the application layer only where deep learning models are deployed and successfully can make detections.
2. The papers directly focus on novel and modern deep learning architectures like LSTM, Convolutional Networks, Autoencoders, etc. that make DDoS detection using a signature detection approach or anomaly detection approach.
3. Our paper highlights the gaps and limitations of these advanced models that still exist and need to be overcome, to truly protect the IoT networks from such kind attacks.

TABLE 1. Summary of Existing Surveys On DDOS Attack Detection

Existing Surveys	Taxonomy of DDoS Attacks	Dynamics of DDoS Attacks	Machine Learning-Based Defense Mechanics	Deep Learning-based Defense Mechanism	Open Challenges and Issues
(Zargar et al. 2013)	✓	✓ (Limited to botnets and malware)	-	-	✓
(Sonar & Upadhyay, 2014)	-	-	-	-	-
(Zhang & Green, 2015)	-	-	✓	-	-
(Yang et al. 2017)	✓	✓ (Limited to botnets and malware)	-	-	-
(Abdul-Ghani et al. 2018)	✓	✓	-	-	✓
(Vishwakarma & Jain, 2020)	✓	✓	✓	✓	✓
(Ferrag et al. 2020)			✓	✓	
(Aleesa et al. 2020)	✓		✓	✓	
(Ahmad et al. 2021)	✓		✓	✓	
(Gamage & Samarabandu, 2020)	✓		✓	✓	
(Ahmad & Alsmadi, 2021)			✓	✓	
(Mittal et al. 2022)	✓	✓	✓	✓	✓
Our Paper	✓	✓	✓	✓	✓

DEEP LEARNING

Deep learning fundamentally is developed on neural networks in the form of interconnected layers of neurons. A neuron is the building block that computes the weighted sum of inputs, determines the bias term, and applies the activation function to determine the intricate relationships contained in the data. With a given vector of data represented as $x = [x_1, x_2, \dots, x_n]$ The weighted sum and activation y can be represented as (Anthony, 2001):

$$z = \sum_{i=1}^n w_i \cdot x_i + b \quad (1)$$

$$y = \sigma(z) \quad (2)$$

Here w_i are the learnable weights used to develop the relationship between inputs and outputs. $\sigma(z)$ is the activation function that infers the non-linear relationships in the model. Numerous types of functions are available

in the literature, where the most commonly employed ones are Sigmoid, Rectified Linear Unit (ReLU), and hyperbolic tangent (tanh). Mathematically, these activation functions are represented as follows (Sharma et al. 2017):

$$\text{Sigmoid: } \sigma(z) = \frac{1}{1+e^{-z}} \quad (3)$$

$$\text{ReLU: } \sigma(z) = \max(0, z) \quad (4)$$

$$\text{tanh: } \sigma(z) = \frac{2}{1+e^{-2z}} - 1 \quad (5)$$

In deep neural networks (DNN) various layers L of neurons are stacked together in the form of input, output, and hidden layers. Output from each of the l^{th} layers is represented as $a^{(l)} = [a_1^{(l)}, a_2^{(l)}, \dots, a_{n_l}^{(l)}]$. Where n_l represents the neurons contained in the l^{th} layer. As a result of forward propagation, the following outcomes are attained:

$$z^{(l)} = W^{(l)} \cdot a^{(l-1)} + b^{(l)} \quad (6)$$

$$a^{(l)} = \sigma(z^{(l)}) \quad (7)$$

Here $W^{(l)}$ represents a weighted matrix which connected l^{th} layers to $l - 1$ layer. Within these deep learning networks are various types including Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs). Both such networks have an innate ability to extract information contained in the dataset. The CNNs excel by processing grid-like data, generally in the form of images through a network of pooling and convolutional layers. These layers make use of kernels (generally termed filters) for scanning the input data along 2D dimensions. Considering XX and K to be the inputs and filters, the feature map Z is generated using the following mathematical model:

$$Z = X * K \quad (8)$$

These feature maps are then processed using pooling layers that aid in dimensionality reduction to capture the desired set of patterns.

The most commonly used method in DDoS attack detection using deep learning, however, is the use of Recurrent Neural Networks (RNNs) like Long Short Term Memory (LSTM). RNNs are used to infer sequential data exhibiting patterns over time series. The feedback loops admissible help processing information across time stamps. Give a sequence of time-series vector $x^{(t)}$, the hidden state of RNN training at each time stamp t can be represented as $h^{(t)}$. The state gets updated with each time stamp as follows:

$$h^{(t)} = \sigma(W_h \cdot h^{(t-1)} + W_x \cdot x^{(t)} + b) \quad (9)$$

The traditional RNNs suffer from a vanishing gradient problem that makes it difficult for them to infer long-term dependencies. LSTM can help address this issue through an architecture of memory cells and gates. Mathematically, LSTM traverses through a series of steps as presented below:

$$i^{(t)} = \sigma(W_i \cdot x^{(t)} + U_i \cdot h^{(t-1)} + b_i) \quad (10)$$

$$f^{(t)} = \sigma(W_f \cdot x^{(t)} + U_f \cdot h^{(t-1)} + b_f) \quad (11)$$

$$o^{(t)} = \sigma(W_o \cdot x^{(t)} + U_o \cdot h^{(t-1)} + b_o) \quad (12)$$

$$c^{(t)} = f^{(t)} \odot c^{(t-1)} + i^{(t)} \odot \tanh(W_c \cdot x^{(t)} + U_c \cdot h^{(t-1)} + b_c) \quad (13)$$

$$h^{(t)} = o^{(t)} \odot \tanh(c^{(t)}) \quad (14)$$

Where i , f , and oo represent the input gate, forget gate, and output gate, respectively. c is the state of a cell, and \odot represents an element-wise multiplication.

The training of a deep learning model involves an identification of the right set of weights and biases. This is attained by the minimization of the loss function $L(\hat{y}, y)$ where \hat{y} and y are the predicted and true labels, respectively. The minimization of the cost function $J(\theta)$ is required which represents the average loss function over the entire dataset. This is represented as:

$$J(\theta) = \frac{1}{m} \sum_{i=1}^m L(\hat{y}^{(i)}, y^{(i)}) \quad (15)$$

A gradient descent algorithm is generally adopted for the minimization of the cost function. The updated weights and biases are computed using the gradient of the cost function as follows:

$$\theta \leftarrow \theta - \alpha \nabla J(\theta) \quad (16)$$

Where α controls the learning rate. The performance of a DDoS attack detection model built upon the deep learning algorithms is determined using several metrics including precision, accuracy, recall, and F1-score. These metrics are derived using true positives (TP), false positives (FP), true negatives (TN), and false negatives (FN).

CONVOLUTIONAL NEURAL NETWORKS (CNNs)

The use of CNNs has emerged as a powerful tool for DDoS attack detection where the inherent capability of CNN architecture is leveraged to explore the hierarchical and intricate structures and patterns contained in the data. Many research articles have been published that demonstrated the ability of CNNs to detect and mitigate DDoS attacks. CNNs along with some of the related techniques like transfer learning are being used in the IoT ecosystems for DDoS attack prevention. This section focuses on examining

some of the methodologies explored under these architectures that can help develop a deeper understanding of the context-aware applications in IoT networks.

A CNN architecture starts with the generation of images for DDoS attacks, where network traffic is transformed into a 2D image representation. Each of the network packets is treated as a frame, to make a time-series representation. These images are then either treated individually or concatenated to make a series representation. The pixels contained in the images are used to infer network details including packet size, type of underlying transfer protocol, IP addresses, etc. The features and trends contained in the data are then inferred by the model to capture attack patterns and anomaly detection. Some of the examples involve the rate of incoming traffic, entropy contained in the packet payload, etc. This translation into images from the traffic data can be made using various models like Short Time Fourier Transform (STFT), Wavelet Transform, or Morlet Transform (a version of wavelets). Having generated these images, the various types of CNN architectures having connected convoluted blocks (convolutional layers, pooling layers, dropout layers, and

fully connected layers), can be deployed. These layers help transform these images into normal or attack classes of data traffic.

One particular technique commonly used in such CNN architecture for attack detection is transfer learning. In this technique, the CNN following numerous architectures is pre-trained on large image datasets including ImageNet, etc. During such training phase, the CNN models learn to extract the hierarchical and abstract features for the input data. This pre-trained architecture is used as a base model, where introductory layers are used to recognize features including edges, textures, shapes, etc. that can aid in the detection of attack patterns. Thus, instead of making a model to learn from scratch, the prior training helps analyze these detections. Such models offer numerous benefits in the form of reduced training time, leveraging the power of features contained in the pre-trained datasets, improved generalization, and handling data imbalance. Some of the commonly used architecture involve ResNets, DenseNets, InceptionNets, etc. An overview of a typical CNN architecture used for DDoS attack detection is presented in the figure below.

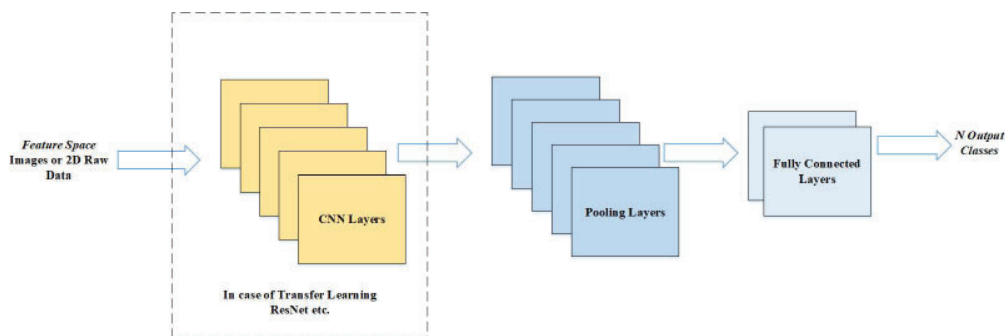


FIGURE 1. CNN Architecture in DDoS Attack Detection

Numerous articles have been published making use of CNN or transfer learning to make DDoS attack detection with higher levels of accuracy. In (Haider et al. 2020), the authors have presented a deep CNN ensemble framework for DDoS attack detection. The model has been tested on three control planes of the software-defined network including the application, control, and data plane. The model has been developed in the form of a deep learning architecture, where multiple types of data are transformed into a concatenated model using CNN layers. These layers are then passed on to an ensemble CNN where the output in the form of attack or normal data is generated. The model has been found to attain an accuracy level of 99.45 percent.

Another article presented in (Cheng et al. 2020) proposed a multiscale CNN architecture, for DDoS attack detection. The method makes use of a grayscale feature matrix, that has proven to offer improved robustness, reduction in the false alarm rate, and outperforms the

existing methods. The accuracy rate of 94.87 has been attained using this combined featured and deep learning approach.

The authors in (F. Hussain et al. 2020) proposed a CNN architecture for DDoS attack detection in IoT networks. The network traffic has been transformed into images and passed through the developed CNN architecture. The architecture makes use of transfer learning by introducing ResNet at the base for making detections. The model has been found to have over 99.99 percent accuracy in making the binary classification i.e. normal vs. attack. Additionally, the model attains an accuracy of 87 percent in creating sub-classification groups where 11 types of DDoS attacks have been detected.

The article presented in (Singh & Jayakumar 2022) introduces a novel framework for DDoS attack detection using two stages. In the first stage, optimal feature selection has been introduced called Improved Update oriented Rider

Optimization Algorithm (IU-ROA). Features generated using this algorithm are fed to a Convolutional Neural Network (CNN) to make classifications into one of the two categories (normal or attack traffic). It has been found that the model attains an accuracy of 96 percent in the detection of attack traffic.

In (B. Hussain et al. 2020), the authors developed a CNN model for DDoS attack detection in 5G cellular networks. The attack data involved simulated traffic that has been generated using silent signaling, SMS spamming, etc. It has been found that the model attains an accuracy of over 91 percent in detecting normal and attack traffic.

RNNS AND LSTM

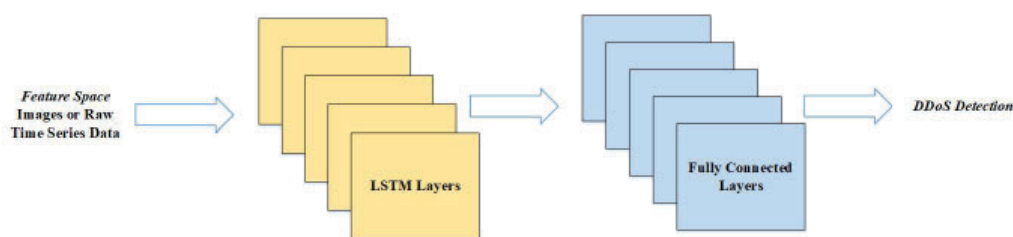
RNNs and LSTM are the advanced architectures for DDoS attack detection that make network data traverse through various steps to infer the attack and normal traffic. Initially, the data is preprocessed into time-series information relating to the packet headers, flow records, etc. The time-series data is transformed into appropriate sequences suitable for RNN/LSTM architecture input. The network traffic data is thus transformed into input-output pairs of sequences, representing specific time windows of the network activity. The frames and window sizes can be adjusted as per the system's architectural requirements. The transformed data then be processed either in raw format or converted into feature space using manual annotations. Some of the features may involve the size of packets, type of protocol, number of packets per second per IP address, etc. Feature selection can be based on domain knowledge and feature engineering. The output labels can be made data categories into some of the known attack types, or general categories of normal and attack sequences.

LSTM with its ability to capture long-term dependencies has been proven to be an effective tool in DDoS attack detection. A typical LSTM model for DDoS attack detection can comprise one or numerous LSTM layers, and fully connected layers.

In the literature, many types of LSTM architecture have successfully been used for DDoS attack detection. One such architecture is known as the vanilla LSTM where sequential data of the network is passed through LSTM cells. The models follow a stacked architecture to detect the patterns contained in the network traffic and classify them into normal or abnormal data patterns. Bidirectional (Bi-LSTM) is an extension to the vanilla LSTM, where features are extracted in the forward and backward directions. This permits the model to capture critical information from the past and future time steps, in a simultaneous manner. Thus bi-directional traversing can help the model to infer complex dependencies contained in the data and can infer highly intricate feature sets to determine the outcomes. In another architecture called Stacked LSTM, the LSTM layers are stacked together to capture the various layers of abstraction contained in the data. This allows the model to extract a hierarchical representation of features contained in the network traffic. This type of architecture is most commonly used in DDoS attack detection with a proven ability to make high-precision classification.

To enhance the performance of the LSTM model, attention mechanisms have been developed that capture the important parts of the input sequence. By allocating weights to relevant parts of the data sequences, the ability of the LSTM model to detect intricate patterns is improved. Another highly efficient model used in LSTM is the use of autoencoders. These are unsupervised learning methods, which aim to construct and reconstruct the input data and output data. Autoencoders can efficiently be used in DDoS attack detection, where normal data is trained to be reconstructed into decoded form. During such reconstructions, higher variations can lead to the anomaly detection.

Apart from the models presented above, there are hybrid LSTM models that are commonly used in DDoS attack detection. These models combine numerous architectures like CNN, Support Vector Machines (SVMs), Random Forest, etc. Such hybrid combinations help detect the complementary features to help enhance the accuracy. The pictorial depiction of various types of models discussed as part of this section has been given in Figure 2:



(a)

continue ...

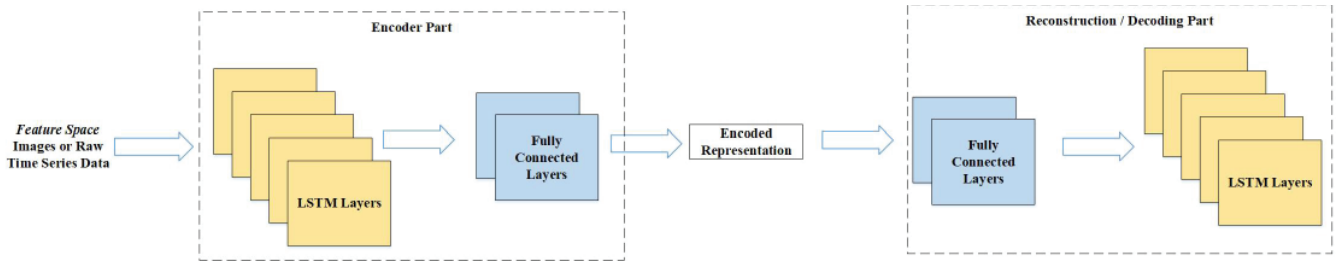


FIGURE 2. LSTM Architectures for DDoS Attack Detection. a. Sequential Architecture. b. Autoencoders

In the (Shurman et al. 2020) a DDoS attack detection model has been developing a sequential LSTM model on a reflection-based dataset. The model comprises multiple LSTM layers stacked together comprising the number of units. The results reveal that the model has attained an accuracy of 92.05% on the training dataset, and 91.54 percent on the test dataset.

In (Dora & Lakshmi 2022), a DDoS attack detection method has been presented that uses a hybrid architecture. The model combines CNN for the feature space extraction, and LSTM for making network data classifications. The optimized feature space has further been selected using the Closest Position-based Grey Wolf Optimization (CP-GWO) algorithm to minimize the correlation between the features extracted using CNN. The model has been found to attain an accuracy of greater than 90 percent for the training and test datasets.

In (Dahiya 2023), the authors have presented a unique DDoS attack detection model that makes use of LSTM and

feature extraction. To attain higher detection rates, Opposition Learning-based Seagull Optimization Algorithm (OLSOA) has been used for model weight optimization. The model attains an overall accuracy of greater than 90 percent for training and test datasets.

In (Bhardwaj et al. 2020), the authors have presented a DDoS attack detection mechanism using autoencoder architecture. The model combines a stacked sparse AutoEncoder for feature extraction coupled using the LSTM deep learning algorithm. This architecture helps make accurate detection of attacks versus normal data traffic. The model attains an accuracy of greater than 90 percent.

In (Sindian & Samer 2020), the authors have presented an improved Deep Sparse Autoencoder for DDoS attack detection. The autoencoder has been developed using LSTM layered architecture and is used for making classifications into normal and attack categories. The model has been found to exhibit an accuracy of 98 percent.

TABLE 2. Summary of the Related Articles on DDoS Attack Detection

Paper Number	Model Type	DDoS Attack Detection	Features Extracted	Model Architecture	Accuracy
(Haider et al. 2020)	CNN Ensemble	✓	✓	Concatenated CNN	99.45%
(Cheng et al. 2020)	Multiscale CNN	✓	✓	CNN	94.87%
(F. Hussain et al. 2020)	CNN	✓	✓ (images)	CNN (Transfer Learning)	99.99%
(Singh & Jayakumar, 2022)	CNN	✓	✓	IU-ROA + CNN	96.00%
(B. Hussain et al. 2020)	CNN	✓	✓	CNN	91.00%
(Shurman et al. 2020)	LSTM	✓	✓	Stacked LSTM	92.05%
(Dora & Lakshmi, 2022)	CNN-LSTM Hybrid	✓	✓	CNN + LSTM	>90.00%
(Dahiya, 2023)	LSTM	✓	✓	OLSOA-Optimized LSTM	>90.00%
(Bhardwaj et al. 2020)	LSTM-Autoencoder	✓	✓	Stacked Autoencoder + LSTM	>90.00%
(Sindian & Samer, 2020)	LSTM-Autoencoder	✓	✓	LSTM Autoencoder	98.00%

RESEARCH GAPS

While we have established the work carried out in the DDoS attack detection using deep learning, some potential gaps exist and shall be made part of future research. Some of these gaps have been discussed below:

STANDARDIZED DATASETS

One of the potential research gaps that exist in DDoS attack detection using deep learning is the lack of standardized datasets. While some of the commonly used datasets involve CICDDoS 2019, and NSL-KDD, however, further diversification is needed to target the evolving nature of the DDoS attacks in IoT networks. Having access to such datasets will help make protection and prevention mechanisms more robust.

HANDLING THE DATA IMBALANCE

The imbalance found in the existing datasets is high since the data points with normal instances are higher than attack instances. This can lead to biased outcomes where detection of attack instances can lead to increasing false negatives. There is a need to handle such data imbalance using data augmentation techniques or simulating the attack instances that closely mimic real-world attack scenarios.

TRANSFER LEARNING

Although some of the studies have focused on transfer learning techniques including ResNet etc. in DDoS attack detection, there is a need to further explore how these pre-trained models can be fine-tuned further to attain higher levels of accuracy and precision. Also, there is a need to explore some of the modern transfer learning architectures like InceptionResnetV2, and Inception V4, etc.

HYBRID ARCHITECTURES

Some of the hybrid architectures developed for DDoS attack detection focus on the combination of CNN and LSTM models. Yet, more combinations are needed to be tested to enhance the accuracy measures.

ADVERSARIAL ATTACKS

As DDoS attacks are getting more sophisticated, therefore, a need to develop robust deep learning models exists to cater to such adversarial attacks. Some of the defense techniques involve robust optimization and enhancement of resilient DDoS detection systems.

CONCLUSION

In this paper, we have discussed the growing concern over DDoS attacks in communication networks, particularly in IoT networks, due to their vast attack surface and limited resources. Traditional rule-based approaches have demonstrated their limitations in coping with the evolving nature of DDoS attacks, leading to an increased interest in deep learning-based solutions. Deep learning models, especially CNN and LSTM architectures, have shown remarkable success in DDoS attack detection, outperforming traditional methods with detection rates exceeding 98%. These models leverage real-world datasets and can adapt to dynamic attack patterns, making them highly effective in mitigating attacks at their inception stages. However, despite the advancements in deep learning-based DDoS detection, several research gaps remain. The lack of standardized datasets, handling imbalanced data, and ensuring real-time detection and scalability are some of the key challenges. Further research is needed to address these gaps and enhance the resilience and explainability of DDoS detection systems. Overall, the integration of deep learning in DDoS attack detection has opened new possibilities for robust and proactive network security. As the landscape of technology continues to evolve, continuous research and innovation are required to stay ahead of the ever-evolving DDoS attack landscape and protect critical communication infrastructures effectively.

ACKNOWLEDGEMENT

The authors would like to thank Universiti Kebangsaan Malaysia for supporting this study.

DECLARATION OF COMPETING INTEREST

None.

REFERENCES

- Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. 2018. A comprehensive IoT attacks survey based on a building-blocked reference model. *International Journal of Advanced Computer Science and Applications* 9(3): 355-373.
- Ahmad, R., & Alsmadi, I. 2021. Machine learning approaches to IoT security: A systematic literature review. *Internet of Things* 14: 100365.
- Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. 2021. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies* 32(1): e4150.
- Aleesa, A., Zaidan, B., Zaidan, A., & Sahar, N. M. (2020). Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions. *Neural Computing and Applications* 32: 9827-9858.
- Anthony, M. 2001. *Discrete Mathematics of Neural Networks: Selected Topics*. SIAM.
- Benkhelifa, E., Welsh, T., & Hamouda, W. 2018. A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. *IEEE Communications Surveys & Tutorials* 20(4): 3496-3509.
- Bhardwaj, A., Mangat, V., & Vig, R. 2020. Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud. *Ieee Access* 8: 181916-181929.
- Bonaccorso, G. 2017. *Machine Learning Algorithms*. Packt Publishing Ltd.
- Cheng, J., Liu, Y., Tang, X., Sheng, V. S., Li, M., & Li, J. 2020. DDoS attack detection via multi-scale convolutional neural network. *Computers, Materials & Continua* 62(3).
- Cook, S. 2023. *20+ DDoS attack statistics and facts for 2018-2023*. comparitech. <https://www.comparitech.com/blog/information-security/ddos-statistics-facts/>
- Dahiya, D. 2023. DDoS attacks detection in 5G networks: hybrid model with statistical and higher-order statistical features. *Cybernetics and Systems* 54(6): 888-913.
- Dora, V. R. S., & Lakshmi, V. N. (2022). Optimal feature selection with CNN-feature learning for DDoS attack detection using meta-heuristic-based LSTM. *International Journal of Intelligent Robotics and Applications* 6(2): 323-349.
- Džaferović, E., Sokol, A., Abd Almisreb, A., & Norzeli, S. M. 2019. DoS and DDoS vulnerability of IoT: A review. *Sustainable Engineering and Innovation* 1(1): 43-48.
- Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications* 50: 102419.
- Gamage, S., & Samarabandu, J. 2020. Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications* 169: 102767.
- Haider, S., Akhuzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K.-K. R., & Iqbal, J. 2020. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. *Ieee Access* 8: 53972-53983.
- Hussain, B., Du, Q., Sun, B., & Han, Z. 2020. Deep learning-based DDoS-attack detection for cyber-physical system over 5G network. *IEEE Transactions on Industrial Informatics* 17(2): 860-870.
- Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. 2020. IoT DoS and DDoS attack detection using ResNet. 2020 IEEE 23rd International Multitopic Conference (INMIC):
- Kaspersky. 2022. *Internet of Things Security Challenges and Best Practices*. Kaspersky. <https://www.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security>
- Kumari, P., & Jain, A. K. 2023. A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, 103096.
- Microsoft. 2023. *2022 in review: DDoS attack trends and insights*. Microsoft. <https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/>
- Mittal, M., Kumar, K., & Behal, S. 2022. Deep learning approaches for detecting DDoS attacks: A systematic review. *Soft Computing*, 1-37.
- Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things* 11: 100227.
- Otoum, Y., & Nayak, A. 2021. As-ids: Anomaly and signature based ids for the internet of things. *Journal of Network and Systems Management* 29: 1-26.
- Pradhan, B., Bhattacharyya, S., & Pal, K. 2021. IoT-based applications in healthcare devices. *Journal of Healthcare Engineering* 2021: 1-18.
- radware. 2021. *Does Your DDoS Protection Solution Defend Against the Latest Attacks?*. radware. <https://www.radware.com/blog/ddos-protection/2021/11/does-your-ddos-protection-solution-defend-against-the-latest-attacks/>
- Rajendran, R., Santhosh Kumar, S., Palanichamy, Y., & Arputharaj, K. 2019. Detection of DoS attacks in cloud networks using intelligent rule based classification system. *Cluster Computing* 22: 423-434.
- Sharma, S., Sharma, S., & Athaiya, A. 2017. Activation functions in neural networks. *Towards Data Sci.* 6(12): 310-316.

- Shrestha, A., & Mahmood, A. 2019. Review of deep learning algorithms and architectures. *Ieee Access* 7: 53040-53065.
- Shurman, M. M., Khrais, R. M., & Yateem, A. A. 2020. DoS and DDoS attack detection using deep learning and IDS. *Int. Arab J. Inf. Technol.* 17(4A): 655-661.
- Sindian, S., & Samer, S. 2020. An enhanced deep autoencoder-based approach for DDoS attack detection. *Wseas Trans. Syst. Control* 15: 716-725.
- Singh, S., & Jayakumar, S. 2022. DDoS attack detection in SDN: optimized deep convolutional neural network with optimal feature set. *Wireless Personal Communications* 125(3): 2781-2797.
- Sonar, K., & Upadhyay, H. 2014. A survey: DDOS attack on Internet of Things. *International Journal of Engineering Research and Development* 10(11): 58-63.
- statistica. 2023. *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025*. statistica. <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>
- Talavera, J. M., Tobón, L. E., Gómez, J. A., Culman, M. A., Aranda, J. M., Parra, D. T., Quiroz, L. A., Hoyos, A., & Garreta, L. E. 2017. Review of IoT applications in agro-industrial and environmental fields. *Computers and Electronics in Agriculture* 142: 283-297.
- Vishwakarma, R., & Jain, A. K. 2020. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems* 73(1): 3-25.
- Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. 2017. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of things Journal* 4(5): 1250-1258.
- Zargar, S. T., Joshi, J., & Tipper, D. 2013. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials* 15(4): 2046-2069.
- Zhang, C., & Green, R. 2015. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. Proceedings of the 18th symposium on communications & networking,