[Array 19 (2023) 100316](https://doi.org/10.1016/j.array.2023.100316)

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Contents lists available at ScienceDirect |  |
| Array |
| journal homepage: [www.sciencedirect.com/journal/array](https://www.sciencedirect.com/journal/array) |

Capturing low-rate DDoS attack based on MQTT protocol in software Defined-IoT environment   
Mustafa Al-Fayoumi, Qasem Abu Al-Haija\*   
*Department of Cybersecurity, Princess Sumaya University for Technology (PSUT), Amman, 11941, Jordan*

|  |  |
| --- | --- |
| A R T I C L E I N F O | A B S T R A C T |
| *Keywords:*  Cybersecurity  Denial-of-service attack (DoS) Software defined network (SDN) Internet of things (IoT)  MQTT protocol | The MQTT (Message Queue Telemetry Transport) protocol has recently been standardized to provide a light-weight open messaging service over low-bandwidth and resource-constrained communication environments. Hence, it is the primary messaging protocol used by Internet of Things (IoT) devices to disseminate telemetry data in a machine-to-machine approach. Despite its advantages in providing reliable, scalable, and timely de-livery, the MQTT protocol is widely vulnerable to flooding and denial of service attacks, specifically, the low-rate distributed denial of services (LR-DDoS). Unlike conventional DDoS, the LR-DDoS attack tends to appear as normal traffic at a very slow rate, which makes it difficult to differentiate from legitimate packets, allowing the packets to move undetected by traditional detection policies. This paper presents an intelligent lightweight detection scheme that can capture LR-DDoS attacks based on MQTT protocol in a software-defined IoT envi-ronment. The proposed scheme examines the performance of four machine learning models on a modern dataset (LRDDoS-MQTT-2022) with a minimum feature set (i.e., two features only) and a balanced dataset, namely: decision tree classifier (DTC), multilayer perceptron (MLP), artificial neural networks (ANN), and naïve Bayes classifier (NBC). Our exploratory assessment demonstrates the arrogance of the DTC detection scheme achieving an accuracy of 99.5% with peak detection speed. Eventually, our best outcomes outdo existing models with higher prediction rates. |

**1. Introduction**

IoT technology is developing quickly, making it possible to use in many fields, such as healthcare, agriculture, manufacturing, and city applications. IoT devices, on the other hand, have limited computing power, storage space, and user interfaces. This makes them vulnerable to security threats. A report from Statistica says that the number of Internet of Things (IoT) devices will triple from 9.7 billion in 2020 to over 29 billion in 2030 [1]. This shows that IoT networks need strong security measures to keep them safe. Fig. 1 shows how the number of IoT devices is expected to grow from 2019 to 2030.

IoT technology can help solve problems without human intervention and can be used to develop smart systems that monitor real-time IoT applications. The IoT architecture comprises various layers, and ensuring interoperability poses a significant challenge. Interoperability can be viewed from different perspectives, such as device, network, syntactic, semantic, and platform interoperability. However, IoT devices can be vulnerable to security attacks, particularly DDoS attacks that disrupt communication between IoT servers and users’ devices [2,3].

The rise of the Internet of Things has opened the door for DDoS at-tackers, who can exploit many insecure devices to create botnets. With new techniques, attackers can launch attacks with minimal bandwidth by taking advantage of vulnerabilities in network devices to amplify their impact on the target system [4,5]. Fig. 2 illustrates a DDoS attack scenario occurring within IoT networks.

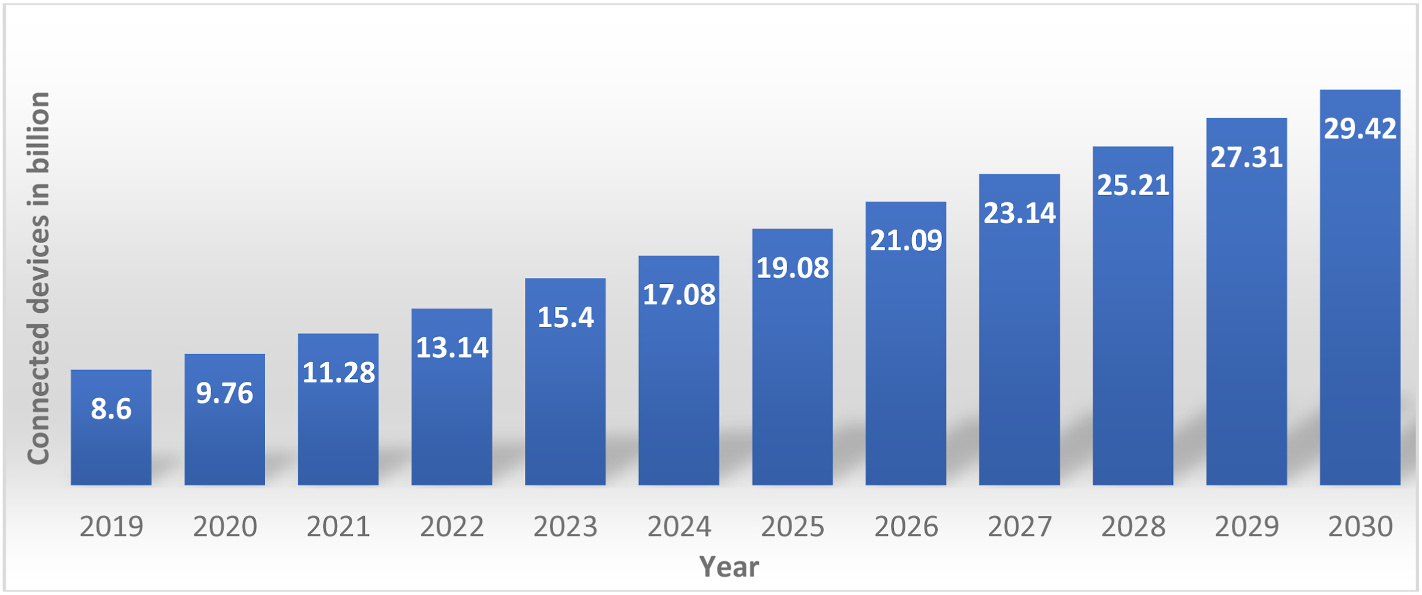
The development of interoperability solutions has enabled the wide deployment of IoT. One of these solutions is Software-Defined Network (SDN), which is referred to as SD-IoT [6,7]. The SDN control layer serves as both a traffic management hub and an Intrusion Detection System (IDS) component to patch security vulnerabilities in IoT networks [8,9]. Furthermore, SDN ensures network interoperability by flexibly man-aging and configuring all heterogeneous equipment in a network. SDN separates the control and data planes. The control plane consists of an SDN controller with network orchestration capabilities, and the data plane comprises network devices responsible for packet forwarding [10]. This approach enhances network agility and scalability while enabling centralized network management. The SDN paradigm has been successful in both wired and wireless networks. In essence, SDN acts as a

\* Corresponding author.

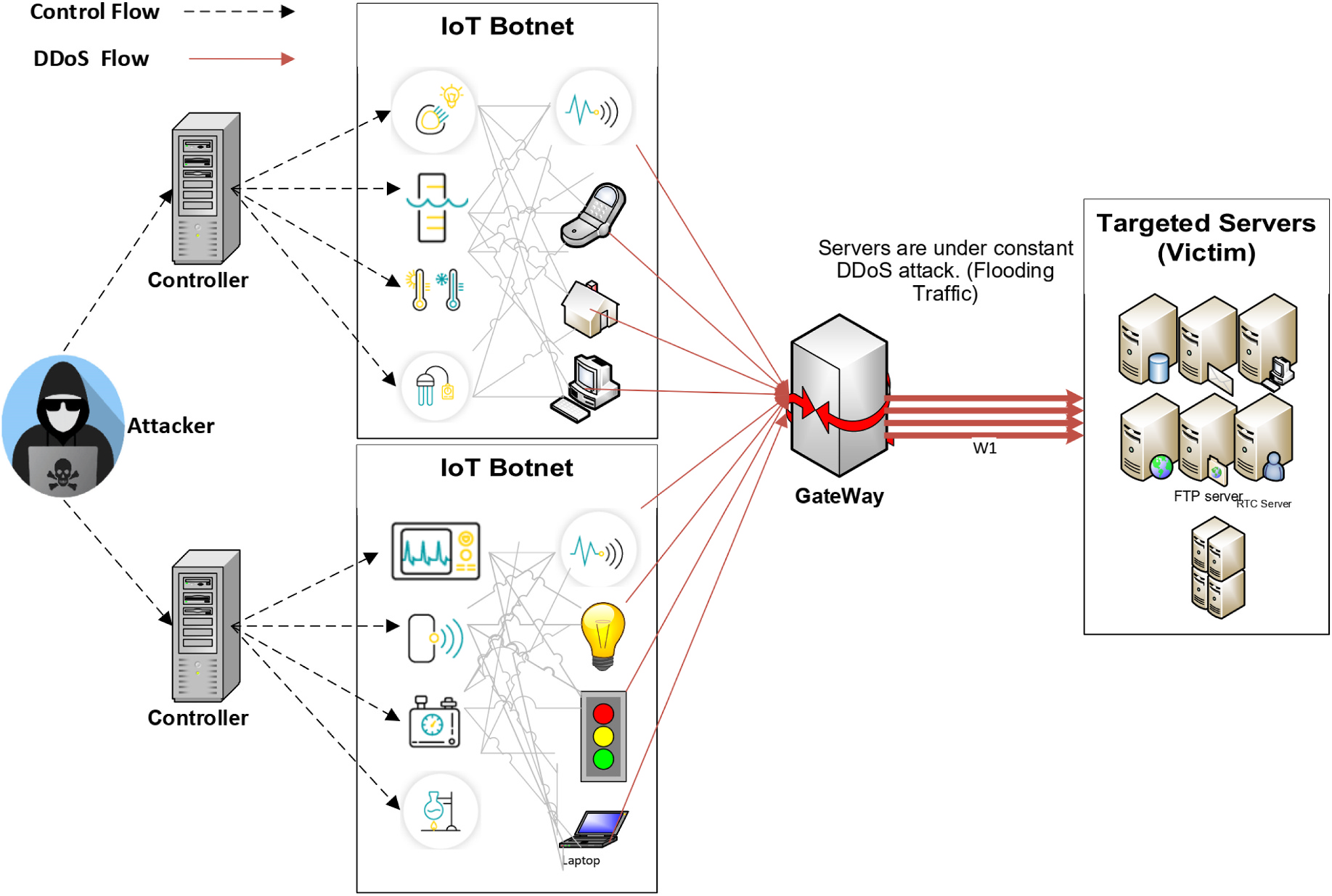
*E-mail addresses:* [m.alfayoumi@psut.edu.jo](mailto:m.alfayoumi@psut.edu.jo) (M. Al-Fayoumi), [q.abualhaija@psut.edu.jo](mailto:q.abualhaija@psut.edu.jo) (Q. Abu Al-Haija).

<https://doi.org/10.1016/j.array.2023.100316>   
[Received 14 March 2023; Received in revised](https://doi.org/10.1016/j.array.2023.100316) form 27 June 2023; Accepted 2 August 2023   
Available online 3 August 2023   
[2590-0056](http://creativecommons.org/licenses/by-nc-nd/4.0/)/© 2023 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*



**Fig. 1.** The predicted increase in IoT devices (2019–2030).



**Fig. 2.** DDoS attack scenario within IoT networks.

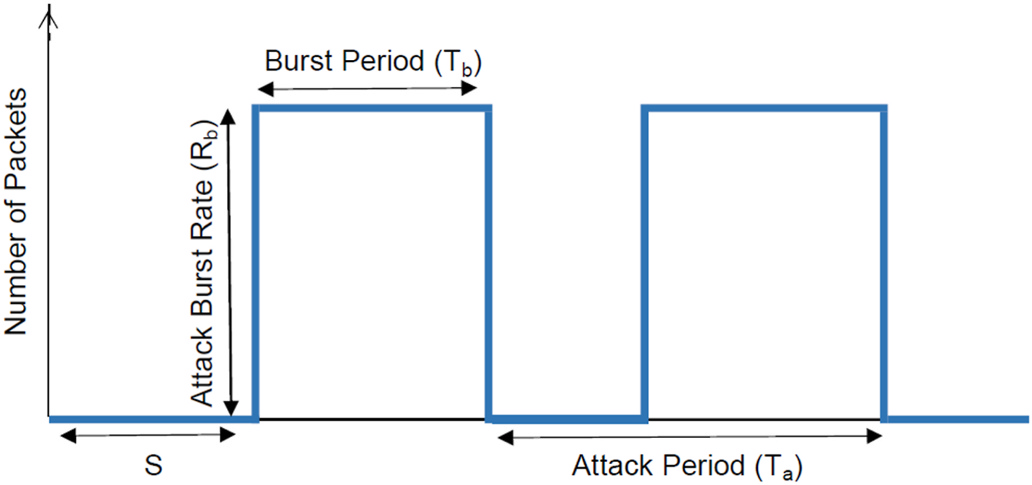
traffic facilitator for the network, managing resources and maintaining IoT network security [11,12].

The SDN structure separates the IoT network’s control and data de-livery functions across distinct abstraction levels. Nevertheless, the centralized control of SDN is still susceptible to DDoS attacks. DDoS attacks are intended to overload the SDN’s centralized management system by continuously sending bogus packets, which can exhaust the computing resources of the controller [13].

Another solution for ensuring interoperability across devices in the IoT perception layer is to utilize the MQTT protocol to handle the het-erogeneous data produced by various smart objects. MQTT is a messaging protocol that allows devices to connect through a central server known as a broker, which is responsible for relaying data from machine to machine. MQTT is based on a publish/subscribe paradigm of operation. However, the widespread adoption of the MQTT protocol has also attracted the attention of cyber attackers who can launch different types of attacks, including LR-DDoS attacks [14]. The LR-DDoS attack is

2

*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*



*1.2. Paper organization*

The remaining parts of this article are structured in the following manner: In Section 2, the literary works are presented and summarized. Section 3 provides the specifics of the proposed scheme, the methodol-ogy for evaluating its efficacy in detecting and preventing Low-Rate DDoS attacks, and details on experiments conducted. Section 4 ana-lyzes the obtained results, compares the implemented schemes, and benchmarks the optical scheme with other state-of-the-art models. Finally, Section 5 concludes the article and suggests potential future directions.

**Fig. 3.** A generic model of LR-DDoS attack. **2. Literature review**

With the increasing number of interconnected IoT devices, LR-DDoS attacks pose a significant challenge to the security and resilience of IoT systems. Fig. 3 illustrates an LR-DDoS attack, including the attack period *Ta*, burst period *Tb*, attack burst rate *Rb*, and starting time *S* [15, 16]. The attack can be identified by analyzing the source, destination IP, port, and protocol. In low-rate TCP DoS attacks, burst packets are sent periodically with a burst rate exceeding the bottleneck capacity, exploiting TCP’s Minimum Retransmission Timeout property. LR-DDoS attacks often use multiple sources with their flow. Zhang et al. [17] categorized these attacks into four groups: Attack Burst Rate Intensifi-cation, Attack Frequency Intensification, Mixed Intensification, and Attack Burst Width Intensification.

Researchers have proposed various detection and mitigation mech-anisms to address the challenge of LR-DDoS attacks on IoT systems. However, only some of these mechanisms could be more efficient or impractical due to the resource constraints of IoT devices [18]. There-fore, there is a need for an effective and efficient mechanism that can detect LR-DDoS attacks based on the MQTT protocol in software-defined IoT environments.

The proposed intelligent lightweight detection scheme can provide a practical defense mechanism against LR-DDoS attacks based on the MQTT protocol. The scheme leverages machine learning techniques to detect LR-DDoS attacks based on minimal features, making it practical for use in resource-constrained IoT devices. By enhancing the security of IoT systems, this research has significant implications for the IoT eco-system’s security and resilience. The main contribution of this paper is an intelligent lightweight detection scheme that can detect LR-DDoS attacks based on MQTT protocol in software-defined IoT environ-ments. This research proposes an efficient and effective approach to tackle the challenges of LR-DDoS attacks that can enhance the security and resilience of IoT systems. The proposed scheme’s simplicity and performance make it suitable for resource-constrained IoT devices and can be integrated into existing security mechanisms to enhance their detection capabilities.

*1.1. Summary of contribution*

This paper employs an AI-based approach to detect LR-DDoS attacks based on MQTT protocol in software-defined IoT environments. This paper’s significant contributions are as follows:

• We propose an intelligent lightweight detection scheme that can provide a practical defense mechanism against LR-DDoS attacks based on the MQTT protocol in software-defined IoT environments. • We implement and assess several machine learning techniques to detect LR-DDoS attacks based on minimal features, making it prac- tical for use in resource-constrained IoT devices. By enhancing the security of IoT systems, this research has significant implications for the IoT ecosystem’s security and resilience.

3

*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*

packages and learning algorithms to develop classifiers that distinguish normal traffic from LR-DDoS attacks. The proposed mechanism demonstrated high accuracy and outperformed traditional solutions.

Nugraha et al. [26] provide a deep-learning architecture for slow DDoS detection. The detection module analyzes SDN switch traffic flow statistics from the SDN controller’s REST API to detect slow DDoS at-tacks. In the detection module, they used a hybrid CNN-LSTM model. This approach was evaluated on custom datasets. The best hyper-parameters optimized the hybrid CNN-LSTM model. This framework used 12 features.

SlowITe is a new low-rate denial-of-service attack proposed by Vaccari et al. [27]. This attack targets MQTT and makes use of low-rate techniques. This study focuses on the vulnerabilities in IoT environ-ments using the MQTT protocol. The authors also explain how the client can modify the Keep-Alive parameter of the server, which gives the attacking node control over the connection closure timeouts on the server. The same authors, Vaccari et al. [28], also introduced SlowTT as an SL-DoS attack. To prevent legitimate clients from setting up MQTT sessions and sending or receiving messages owing to a lack of open connection sockets, the attack aims to consume and block as many of the broker’s open TCP connections as possible. Once the attacker has started a conversation with the broker, they use the MQTT protocol’s network configuration settings, particularly the KeepAlive parameter, to main-tain connections for a long time. By mimicking actual behavior using PINGREQ and PINGRESP packets, SlowTT may also sustain connections for a long time, even with lower KeepAlive levels.

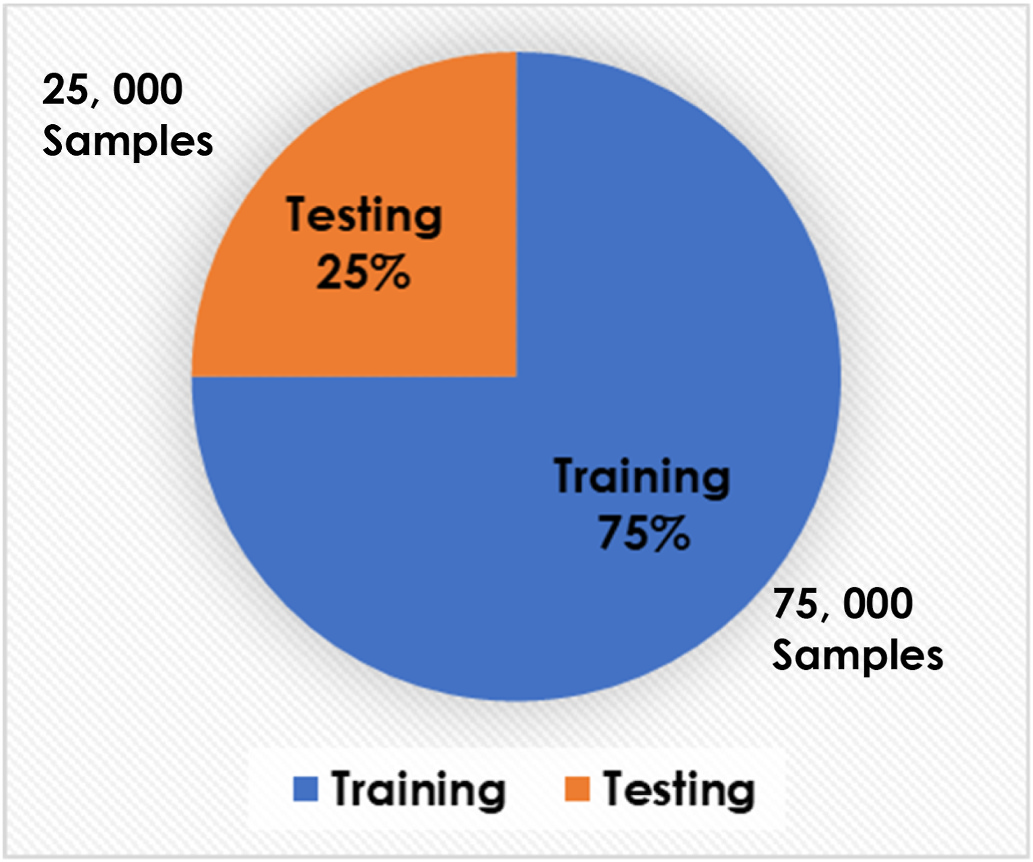
A method for detecting LR-DoS attacks using hybrid deep neural networks that are comprised of a 1-D convolutional neural network and the recurrent gated unit is proposed by Xu et al. [29]. This method uses hybrid deep neural networks. The approach requires temporal statistics of network traffic to detect LR-DoS attacks. Real, legitimate traffic from a website was recorded in a data center, and several low-resource denial-of-service attacks were carried out in a laboratory environment on a copy of the website to record attack traffic. This was done so that the effectiveness of the proposed method could be evaluated. Nada et al. [30]used a novel dataset approach in the emulation procedure. Out of the original 21 features, the experiment also used feature selection using the logistic regression coefficient, producing eight features. For LR-DDoS prediction, the Random Forest (RF) approach was used. For packets sent at 200 packets per second, the accuracy was 98.7%, while the forecast loss value was 99.1%. (PPS).

AlMasri et al. [31] suggest a new method for identifying and pre-venting network attacks using ML techniques. The strategy involves using the NSL-KDD dataset to create a machine-learning system to recognize DoS and port scanning attacks. The method also integrates the results of the ML algorithm with a proven SDN architecture, which should enhance performance by leveraging several previously tried and true procedures. The categorical data were converted into non-categorical data using one-hot encoding as part of the data pre-processing, and the features were chosen using the ANOVA test. Various classifiers were examined using the original dataset and the chosen features from the ANOVA test. The Naive Bayes model delivered the most accurate outcomes. They are using the packet drop method. REPD is a Renyi entropy DDoS attack detection method that Ahalawat et al. [32] suggested. Using the packet-drop technique for prevention, evaluating the probability distribution of flow fluctuations, and achieving better results than the Shannon entropy is possible.

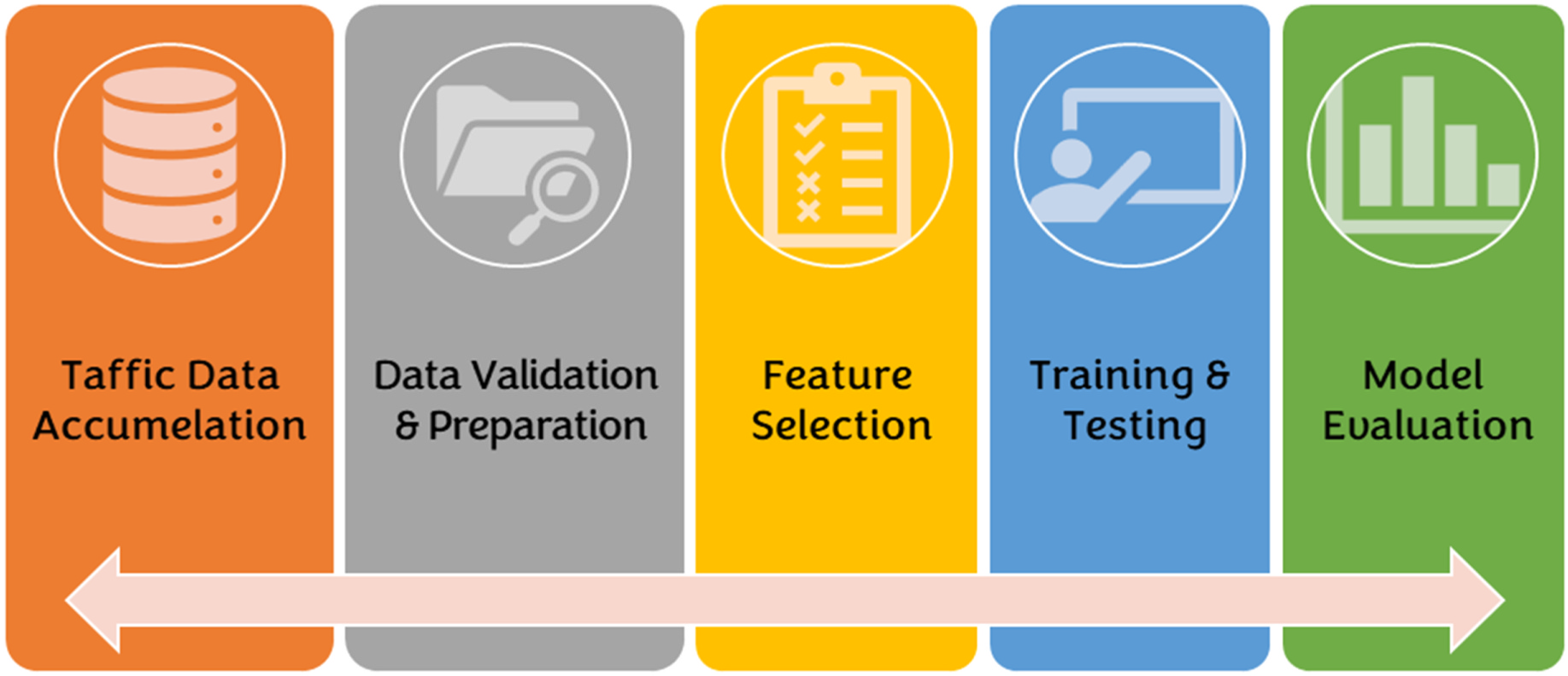
*2.2. DDoS attack based on MQTT protocol in -IoT environment*

In IoT networks, the MQTT protocol is used for machine-to-machine communication, making it vulnerable to DDoS attacks. In the study by Haripriya and Kulothungan [33], they found that spoofing attacks can be used against MQTT. This means an attacker can send a malicious packet that looks like a legitimate message packet. This vulnerability happens because the MQTT broker can’t tell the difference between

4



*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*



**Fig. 4.** Overall workflow diagram for developing and evaluating the proposed LR-DDoS detection system.

to lessen the threat. The proposed technique rapidly identifies and mitigates the DDoS attack by removing the flow entry from the switch using monitoring data acquired from flows and state tables at the data plan. The drawback of this strategy is that the switch needs to inform the controller of the states when the window size is too large. Anbarsu et al. [40] proposed a fuzzy logic-based IDS with deep neural networks (DNNs) in an SDN network to detect DDoS attacks. The combination of fuzzy logic and DNNs is motivated by their high classification accuracy and low false positive rate. The proposed IDS was evaluated using the “KDD CUP99″ dataset. However, implementing deep learning algo-rithms requires expensive GPUs and specialized knowledge. Ivanova et al. [41] developed a feed-forward neural network model to recognize DoS and DDoS attacks that use various activities. When the model was put through its paces using the BotIoT dataset, it effectively detected DDoS attacks using 8 or 10 features, attaining an accuracy rate of 99.99% overall. The Adam optimization technique and a hyperbolic tangent activation function are used for each neuron in the neural net-work’s single hidden layer.

The literature review highlights the knowledge gap in detecting LR- DDoS attacks based on MQTT protocol in SD-IoT environments using lightweight and efficient detection mechanisms. While previous studies proposed detection mechanisms, they require significant resources or could perform better on resource-constrained IoT devices. Additionally, few studies have explored the feasibility and effectiveness of ML-based detection mechanisms for LR-DDoS attacks based on the MQTT proto-col. Therefore, the article proposes an intelligent lightweight detection scheme that uses machine learning models and minimal features to achieve high detection accuracy with peak detection speed. To the best of our knowledge, this study is the first ML-based study to use only two features and achieve the best accuracy with maximum detection speed compared to previous works.

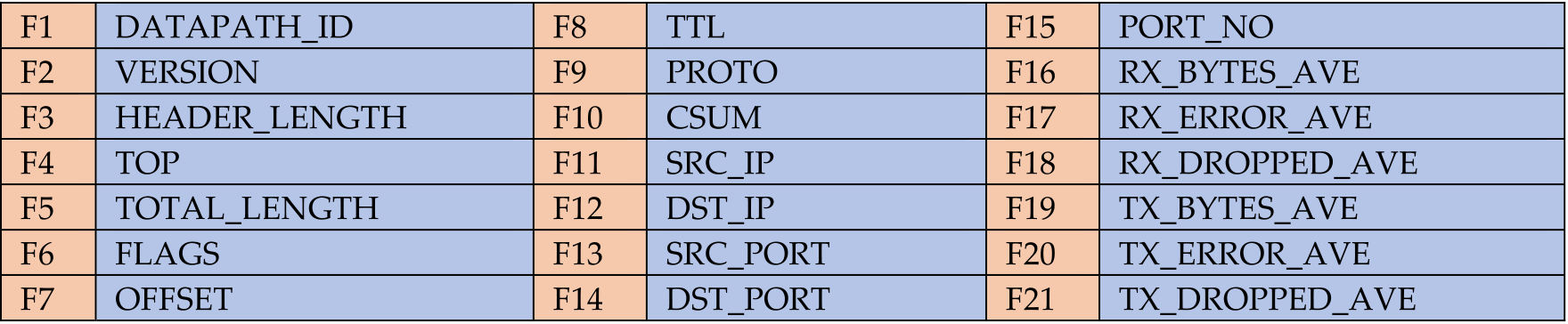
|  |  |  |
| --- | --- | --- |
|  |  |  |

**Fig. 6.** Dataset distribution statistics.

**3. LR DDoS recognition methodology**

This section uses various learning and evaluation techniques to investigate the development and assessment approaches of the proposed low-rate DDoS attack detection model based on the MQTT protocol in the software-defined Internet of Things environment (SDN-IoT). Fig. 4 illustrates the overall workflow diagram for developing and evaluating the proposed LR-DDoS detection system.

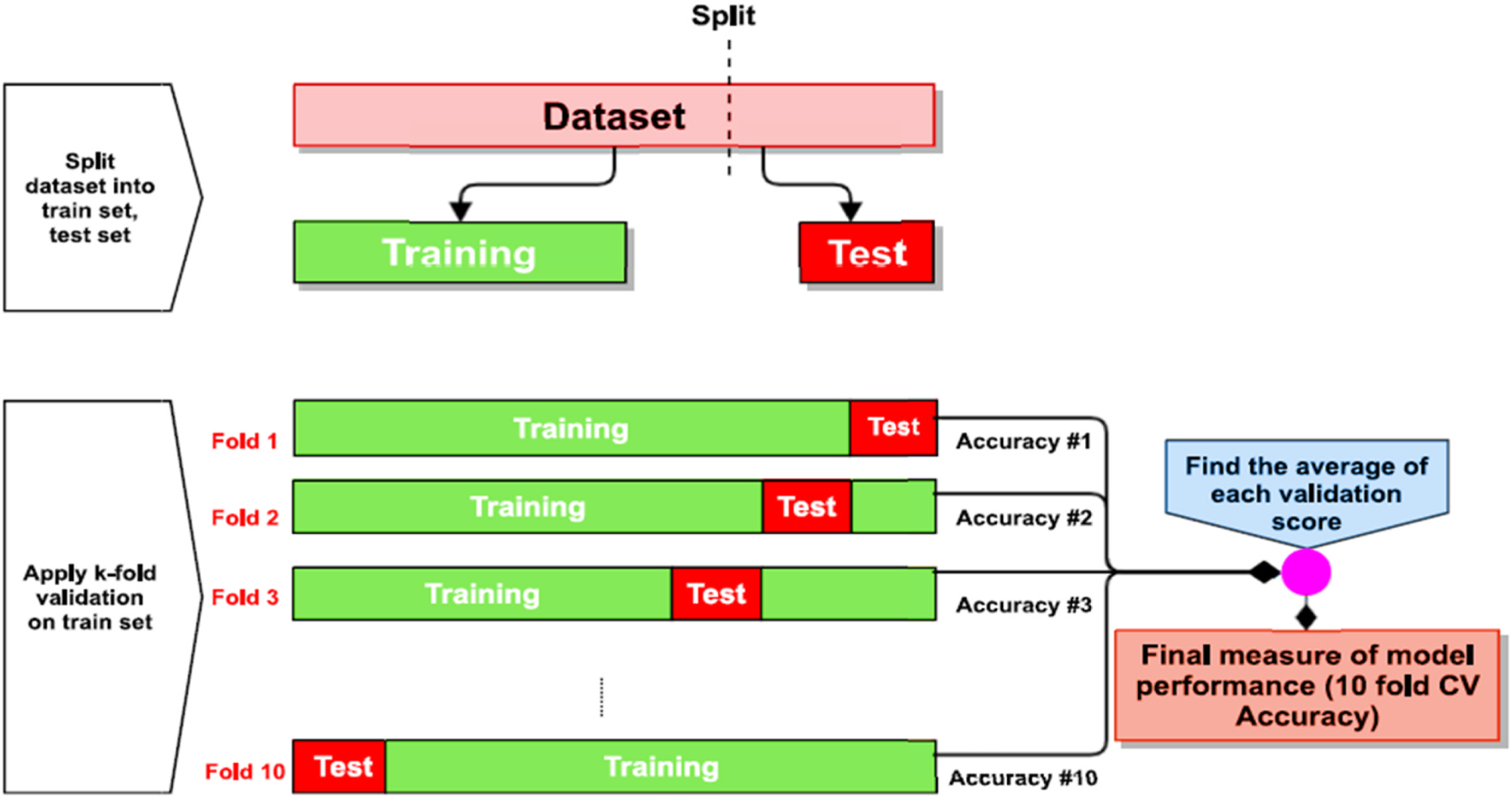
Initially, the traffic data was accumulated from the Mendeley data



**Fig. 5.** Feature set in the original dataset (LR-DDoS-MQQT-2022 dataset [30]).

5

*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*



**Fig. 7.** Ten-fold cross-validation diagram [42].

repository, a global data warehouse for different applications and dis-ciplines. LR-DDoS-MQQT-2022 dataset [30] has been collected for the purpose of model evaluation in capturing LR-DDoS attacks based on MQQT protocol in a software-defined IoT environment. LR-DDoS-MQQT-2022 dataset is an up-to-date and balanced dataset that has been extracted using the OpenFlow software tool for generating real-time DDoS attacks in SD-IoT. It comprises 200,00 traffic samples distributed equally into two target classes: 100,00 samples for the normal traffic and 100,00 samples for the LR-DDoS traffic. Besides, its feature set comprises 21 input features (shown below in Fig. 5) and one label feature used to classify the traffic as normal or LR-DDoS.

After that, the accumulated dataset underwent a validation and preparation phase to ensure the readiness of the traffic samples for the training procedure using the machine learning modules. This includes the samples checking against missing records/values, duplicated sam-ples, errors in data entries, categorical data encoding or excluding samples randomization, and the dataset division into training and testing datasets. Fig. 6 shows the distribution of the LR-DDoS-MQQT- 2022 dataset into training and testing datasets.

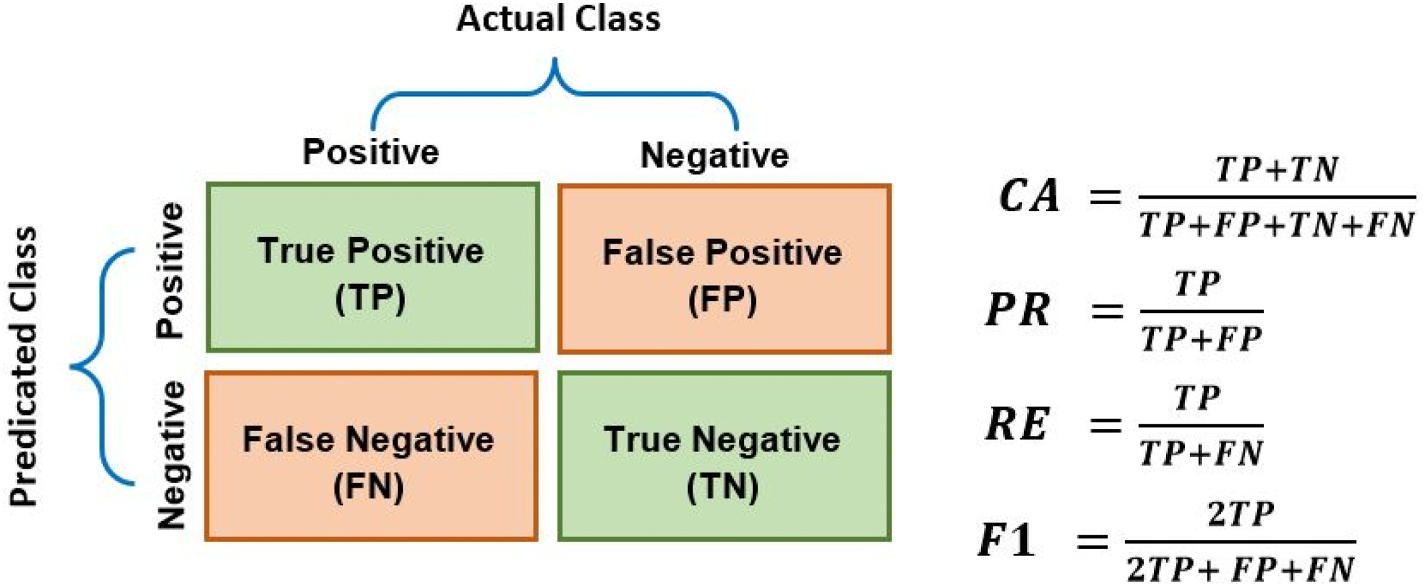
Once the dataset was ready for training/testing phases, we examined all features to extract those essential features in which the system per-formed with the highest performance metrics and the lowest prediction delay. The feature set has undergone a series of feature extraction ex-periments using principal component analysis (PCA) to pick up the

minimum number of essential features that enable the prediction at the highest accuracy and maximum prediction speed (i.e., lightweight). As a result, only two main features (CSUM and SRC\_PORT) have been finally used to develop the proposed lightweight detection system to capture the LR-DDoS attack based on MQTT protocol in software defined-IoT ecosystems.

The next stage is the learning stage which comprises the training and testing phases for the system using the prescribed training and testing datasets. In this module, we have examined the performance ability of four machine-learning models in discovering anomalous traffic, viz. decision tree classifier (DTC), multilayer perceptron (MLP), artificial neural networks (ANN), and naïve Bayes classifier (NBC). At each experiment, we employed the Ten-fold cross-validation in order to ensure effective validation for the learning process using the LR-DDoS- MQQT-2022 dataset. Fig. 7 shows the validation policy used in this research. The dataset was divided into ten parts; nine were taken to train the model, and one was used to test the model. The mean value E of the ten-fold test results is calculated to approximate the model accuracy for the current Ten-fold cross-validation model, where Ei represents the cross-validation error of the ith group.

**4. LR DDoS recognition assessment**

In order to select the best ML mode that provides the best



**Fig. 8.** Evaluation factors [43].

6

*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*

**Table 1**

Summary of review-related research.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model | Method/Architecture | No. of  Features | Advantages | Limitation |
| Mugunthan et al. [19] | RFC model | 41 | • Can detect and prevent low-rate DDoS attacks. • Uses multiple soft computing techniques to increase the accuracy and efficiency  • A novel approach for preventing IP spoofing attacks. | • Could be a concern for real-world implementation. • Lacks extensive experimental results to prove the system’s efficacy.  • Have limitations in terms of scalability and   generalizability to diverse types of networks and  systems.  • Not extremely fast  • Does not discuss the computational and storage requirements of the proposed approach.  • Not extremely fast  • Selecting a large number of features can lead to an increase in both detection and training time. |
| Singh et al. [20] | ABC-ANN | 21 |
| Zhijun et al. [21] | FM/CNN/RFC | 64 | • Several datasets were evaluated.  • Good detection rate with low FP • Able to identify low-rate DDOS.  • Possibility to choose a threshold value based on network traffic conditions.  • High accuracy in detecting DDoS attacks while maintaining low false positive rates  • High-precision and recall LR-DDoS detection and mitigation.  • Flexible and scalable architecture allows seamless integration with existing network  infrastructures.  • High accuracy in detecting LR-DDoS attacks |
| Verma et al. [22] | MAD-RF | 43 |
| P´erez et al. [24] | MLP/SVM | 44 | • Selecting a large number of features can lead to an increase in both detection and training time. |
| Cheng et al. [25] | SVM | 19 | • Limited dataset (Small dataset)  • The proposed approach may require a significant amount of computation, which could pose a  challenge in resource-constrained IoT  environments  • There is a small dataset available to evaluate the effectiveness of the deep learning model. |
| Nugraha et al. [26] | CNN-LSTM | 12 | • The hyperparameters optimized the hybrid CNN-LSTM model.  • High accuracy and low false-positive rates • Behaves as a legitimate traffic |
| Vaccari et al. [27] | SlowITe DDoS attack. Exploit MQTT client-server vulnerability  (connection-closure timeout)  SlowTT DDoS attack. Exploiting the broker’s “Keep-Alive” parameter.  1-CNN-GRU | N\A | • Can be detected if investigated properly |
| Vaccari et al.  [28]  Xu et al. [29] | N\A | • Efficient way of launching a DDoS attack. • Can target a large number of IoT networks • Low-rate detection with high results   (accuracy, precision, recall, and F1-score)  • Detection of LR-DDoS attacks with high re-sults (accuracy, precision, recall, and F1-  score)  • Decreased false negative rate and reduced missed detection rate of LR-DDoS attacks.  • The system employs both unsupervised and supervised machine learning algorithms.  • Using Anova for feature selection achieved high accuracy in detecting Probe attacks.  • Used packet drop method for mitigation. • Can detect low-rate DDoS | • Can be detected if investigated properly |
| NA | • Not extremely fast |
| Nada et al. [30] | NBC Model | 8 | • Not extremely fast (Training Time (s): 0.422 s) |
| AlMasri et al. [31] | 13 | • Low accuracy in detecting DoS attacks.  • Selecting a large number of features can lead to an increase in both detection and training time. |
| Ahalawat et al. [32] | Renyi Entropy with Packet Drop “REPD" DDoS attack detection technique  Fuzzy logic-based approach | NA | • Not extremely fast. |
| Haripriya et al. [33] | 2 | • Fast approach | • It is unclear how the input parameters Connection Message Ratio (CMR) and Connection  Acknowledgement Message Ratio (CAMR) were determined.  • Using a common information-based feature selec- tion method  • High computational Complexity: It requires a long time (*>*1 min) of data-gathering to perform better.  • The proposed models are evaluated only on a specific scenario (smart home) and may not  generalize well to other scenarios or applications.  • Complex model that requires resources |
| Kumar et al.  [34]  Ghannadrad [36] | RF/Fog computing-based distributed intrusion detection framework  RF, KNN, &  SVM with ANOVA as FS/Realistic MQTT dataset with benign and  malicious flow-level  communications.  CNN-LTSM | 10 | • Uses a few parameters and can be updated in real-time deployment.  • binary and multi-level classification was used for differentiating between malicious and  legitimate traffic |
| 10 |
| Aldhyani et al. [37] | 29 | • High intrusion detection accuracy. Accuracy is 98.9%, Precision is 99.2%, The recall is  99%, F1-score is 99.1%  • High detection rate from 98% to 100% with low False-Positive.  • Several IoT nodes and packet sizes were used. • IoT-based stateful SDN DoS and DDoS   detection and mitigation.  • Quickly detects and prevents real-time DDoS attacks.  • The detection rate is between 80% and 100% based on the window size. |
| Bhayo et al. [38] | A framework was developed to improve the DDoS detection accuracy.  entropy-based method for detecting and mitigating DDoS attacks based on OpenState protocol | 6 | • Complex and heavy model |
| Galeano-   Brajones et al.  [39] | 4 | • It may require significant computational resources to implement, which could limit its practicality for  resource-constrained IoT devices.  • It stops responding to the controller regarding the states when the window size is too large.  • The experimental setup used in the study is small, limiting the results’ generalizability to larger-scale  IoT networks.  • Requires expensive GPUs and specialized knowledge. |
| Anbarsu et al. [40] | Fuzzy logic-based IDS with Deep Neural Networks | 6 | • Good classification accuracy and low False Positive Rate |

(*continued on next page*)

7

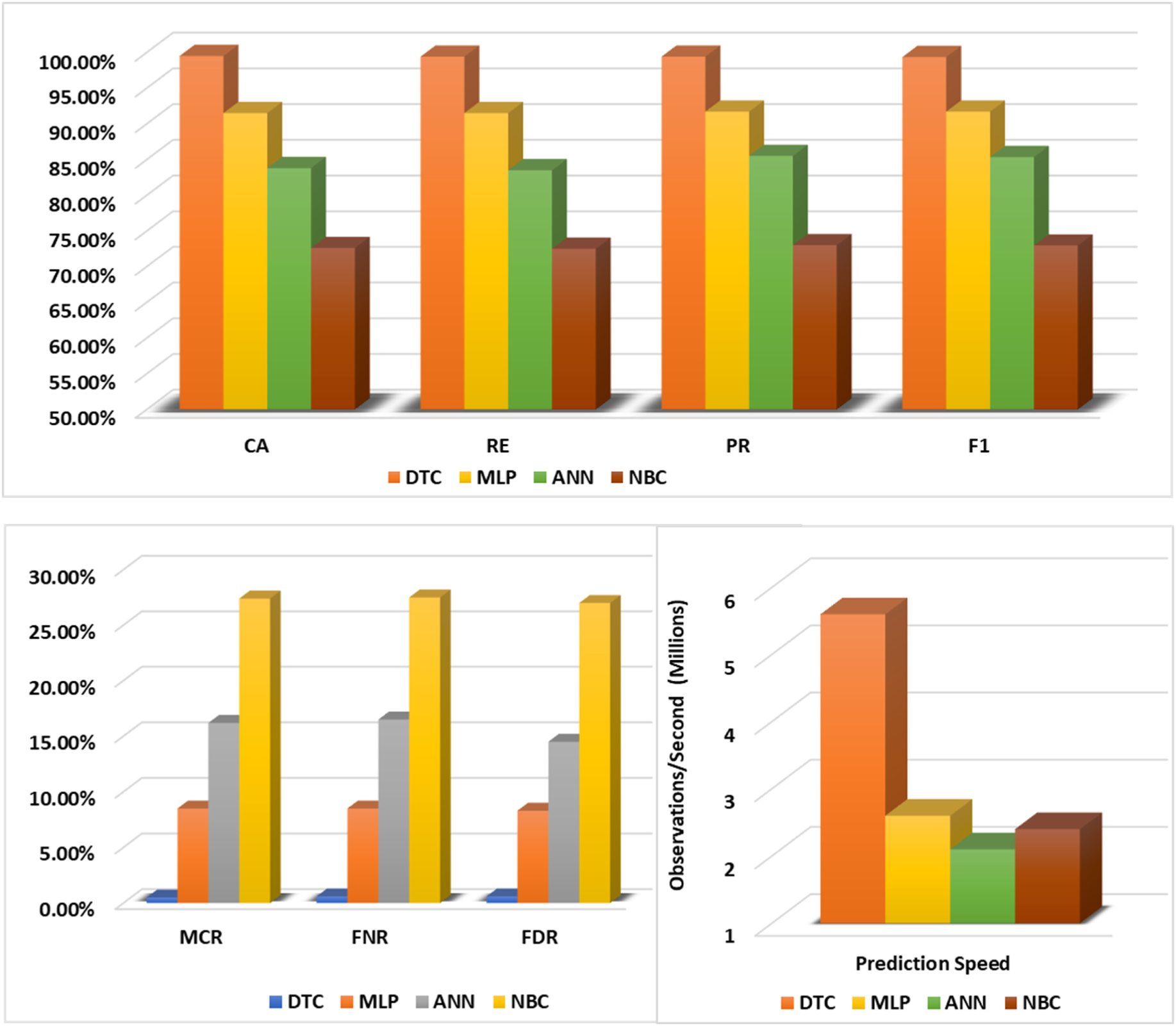
*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*

**Table 1** (*continued*)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model | Method/Architecture | No. of  Features | Advantages | Limitation |
| Ivanova et al. [41] | RNN, Adam optimization, hyperbolic tangent activation function | 10 and 8 | • Distinguish TCP, UDP, HTTP flood,  keylogging, data exfiltration, OS  fingerprinting, and service scan threats from typical network traffic.  • Precision, Recall, F1, and CA is 99.9% | • The accuracy is 92%  • Neural networks are not always able to accurately detect and identify complex patterns and can be  prone to overfitting |

**Table 2**   
System evaluation using three machine learning techniques: DT, SVM, and NB, and in terms of classification accuracy, precision, recall, F1 score, MCR, FNR, FDR, and the prediction speed.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Model | CA | RE | PR | F1 | MCR | FNR | FDR | PRS |
| DTC  MLP  ANN  NBC | 99.5%  91.5%  83.8%  72.6% | 99.4%  91.5%  83.5%  72.5% | 99.4%  91.7%  85.5%  73.0% | 99.35%  91.70%  85.35%  72.95% | 0.50%  8.50%  16.20%  27.40% | 0.60%  8.50%  16.50%  27.50% | 0.60%  8.30%  14.50%  27.00% | 5600000 obs/sec 2600000 obs/sec 2100000 obs/sec 2400000 obs/sec |



**Fig. 9.** System evaluation using three machine learning techniques: DT, SVM, and NB, and in terms of (a) Performance indicators (accuracy, precision, recall, F1 score), (b) False rates (MCR, FNR, FDR), and the prediction speed.

performance indicators and thus can be finally deployed to capture the anomalous LR-DDoS traffic packets, the following performance metrics have been used: classification accuracy rate (CA), true positive rate (TPR) A.K.A recall (RE), positive predictive value (PPV) A.K.A precision

8

*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*

**Table 3**   
Comparing detection accuracy with existing models for LR-DDoS/DDoS attacks detection.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Model | Method | No. of Features | CA | F1 |
| Mugunthan et al. [19] Singh et al. [20]  Zhijun et al. [21]  Zhijun et al. [21]  Zhijun et al. [21]  Verma et al. [22]  P´erez et al. [24]  P´erez et al. [24]  Xu et al. [29]  AlMasri et al. [31]  This work | RFC model ABC-ANN  FM model  CNN model RFC model MAD-RF  MLP Model SVM Model 1-CNN-GRU NBC Model DTC model | 41  21  64  64  64  43  80  80  NA  43  2 | 97.34% 78.50% 95.80% 90.90% 90.30% 60.00% 95.00% 93.10% 98.68% 86.90% 99.50% | 95.45% 57.75% 94.80% 90.30% 88.80% 76.00% 94.98% 93.00% NA  NA  99.35% |

number of observations (samples) per second; this metric particularly generated by MATLAB. The following figure, Fig. 8, summarizes the stated metrics with their equations.

— Classification Accuracy (CA): This performance indicator can be defined as the proportion of correctly classified samples (either positive or negative) among the overall number of samples.

— Classification Recall (Re): This performance indicator is the proportion of actual positive samples correctly (only positive) identified by the system out of all the positive samples in the dataset.

— Classification Precision (PR): This performance indicator can be defined as the proportion of correctly predicted positive samples out of all instances predicted as positive by the system.

— Classification F1 Score (F1): This performance indicator can be defined as the balanced proportion of precision and recall measuring the system’s effectiveness by considering the ability to correctly identify positive samples (precision) and the ability to avoid false negative samples (recall).

— Misclassification Rate (MCR): This performance indicator can be defined as the proportion of incorrectly classified samples (either positive or negative) among the overall number of samples.

— False Negative Rate (FNR): This performance indicator is the proportion of actual positive samples incorrectly (only positive) identified by the system out of all the positive samples in the dataset.

— False Discovery Rate (FDR): This performance indicator can be defined as the proportion of incorrectly predicted positive sam-ples out of all instances predicted as positive by the system.

— Prediction Speed (PRS): This performance indicator can be defined as the number of predictions (observations) that can be performed by the model in 1 s (see Table 1).

Furthermore, Table 2 and Fig. 9 present the system evaluation using three machine learning techniques: DT, SVM, and NB, regarding clas-sification accuracy, precision, recall, F1 score, MCR, FNR, FDR, and prediction speed (PRS). Based on the table and figure results, we can plainly observe the advantage of the DTC model over other models in terms of all performance statistics. It is a high-performant model since it can predict individual communication traffic accurately with 99.5%. It’s also lightweight since it can predict individual communication traffic rapidly with only 179 ns. Besides, it exhibits the least false alarm rates (MCR, FNR, FDR)among all models. Such outcomes indicate the robustness of the model being deployed to work in the real-time appli-cations of the SDN-IoT ecosystem.

Lastly, Table 3 compares the detection accuracy of our DTC-based detection model with existing models for LR-DDoS/DDoS attacks detection in IoT ecosystems. Diverse models were developed and pro-posed to detect the LR-DDoS/DDoS attack detection in IoT ecosystems. To benchmark our results and show the advantages of our lightweight

9

*M. Al-Fayoumi and Q. Abu Al-Haija*  *Array 19 (2023) 100316*

**References**

[1] IoT connected devices worldwide 2019-2030 | Statista.” [Online]. Available: [htt](https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/) [ps://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/](https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/).

[[Accessed: 7-March-2023].](https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/)

[2] [Dantas Silva FS, Silva E, Neto EP, Lemos M, Venancio Neto AJ, Esposito F.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref2)

[A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref2) [IoT scenarios. Sensors 2020;20(11). MDPI AG.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref2)

[3] [Abu Al-Haija Q, Al Badawi A, Bojja GR. Boost-](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref2)Defence for resilient IoT networks: a head-to-toe approach. Expet Syst 2022;39(10):e12934. [https://doi.org/10.1111/](https://doi.org/10.1111/exsy.12934) [exsy.12934](https://doi.org/10.1111/exsy.12934).

[4] [Liu G, Qua](https://doi.org/10.1111/exsy.12934)[n W, Cheng N, Zhang H, Yu S. Efficient DDoS attacks mitigation fo](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref4)r [stateful forwarding in Internet of Things. J Netw Comput Appl 2019;130(June](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref4) [2018):1–13.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref4)

[5] [Faek R, Al-Fawa’reh M, Al-Fayoumi M. Exposing bot attacks using machine](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref5) [learning and flow level analysis. In: International conference on data science, vol.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref5) [2021. E-learning and Information Systems; 2021. p. 99–106.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref5)

[6] [Wang J, Liu Y, Su W, Feng H. A DDoS attack detection base](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref5)[d on deep learning in](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref6) [software-defined Internet of things. In: IEEE vehicular technology conference, vol](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref6). [2020; 2020. p. 7–11.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref6)

[7] [Tuan NN, Hung PH,](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref6) [Nghia ND, Van Tho N, Van Phan T, Thanh NH. A DDoS attack](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref7) [mitigation scheme in ISP networks using machine learning based on SDN.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref7)

[Electronics (Switzerland) 2020;9(3):1–19.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref7)

[8] [Al-Fayoumi M, Ahmad Y, Tariq U. A hete](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref7)[rogeneous framework to detect intruder](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref8) [attacks in wireless sensor networks. Int J Adv Comput Sci Appl 2017;7(12):52–8.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref8)

[9] [Al-Fawa’reh M, Al-Fayoumi M, Nashwan S, Fraihat S. Cyber threat intelligence](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref8) [using PCA-DNN model to detect abnormal network behavior. Egypt Inf J Jul. 2022;](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref9) [23(2):173–85.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref9)

[10] [Abu Al-Haija](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref9) Q, Al-Badawi A. Attack-aware IoT network traffic routing leveraging ensemble learning. Sensors 2022;22:241. <https://doi.org/10.3390/s22010241>.

[11] [Karmakar KK, Varadharajan V, Nepal S, T](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref11)[upakula U. SDN-enabled secure IoT](https://doi.org/10.3390/s22010241) [architecture. IEEE Internet Things J 2021;8(8):6549–64.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref11)

[12] [Li J, Cheng Y. Design and implementation of voice-contr](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref11)[olled intelligent fan system](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref12) [based on machine learning. In: Proceedings of 2020 IEEE international conference](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref12) [on advances in electrical engineering and computer applications. AEECA 2020;](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref12) [2020. p. 548–52.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref12)

[13] [Hakiri A, Bertho](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref12)[u P, Gokhale A, Abdellatif S. Publish/subscribe-enabled software](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref13) [defined networking for efficient and scalable IoT communications. IEEE Commun](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref13) [Mag Sep. 2015;53(9):48–54.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref13)

[14] [Al-Haija QA, McCurry CD, Z](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref13)ein-Sabatto S. Intelligent self-reliant cyber-attacks detection and classification system for IoT communication using deep   
convolutional neural network. In: Ghita B, Shiaeles S, editors. Selected papers from the 12th international networking conference. INC 2020. Lecture notes in networks and systems, vol. 180. Cham: Springer; 2021. [https://doi.org/10.1007/978-3-030-](https://doi.org/10.1007/978-3-030-64758-2_8) [64758-2\_8](https://doi.org/10.1007/978-3-030-64758-2_8).

[15] [Kandoi R,](https://doi.org/10.1007/978-3-030-64758-2_8) [Antikainen M. Denial-of-service attacks in OpenFlow SDN networks. In:](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref15) [Proceedings of the 2015 IFIP/IEEE international symposium on integrated network](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref15) [management. IM 2015; 2015. p. 1322–6.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref15)

[16] [Zhang C, Cai Z, Chen W, Luo X, Yin J. Flo](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref15)[w level detection and filtering of low-rat](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref16)e [DDoS. Comput Network 2012;56(15):3417–31.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref16)

[17] [Tarasov Y, Pakulova E, Basov O. Modeling of](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref16) [low-rate DDoS-attacks. In: ACM](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref17) [international conference proceeding series; 2019. p. 10–3.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref17)

[18] [Ibrahim RF, Abu Al-Haija Q, Ahmad A. DDoS attack prev](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref17)ention for Internet of thing devices using ethereum blockchain technology. Sensors 2022;22:6806.

<https://doi.org/10.3390/s22186806>.

[19] [M SR. Soft computing based autonomous low rate Ddos attack detection and](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref19) [security for cloud computing. J Soft Comput Paradigm 2019;2019(2):80–90.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref19)

[20] [Singh R, Thakur K, Singh G, Gupta S. Prevention of IP spoofing attack in c](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref19)[yber](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref20) [using artificial bee colony and artificial neural network. In: ACM internationa](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref20)l [conference proceeding series; 2019.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref20)

[21] [Zhijun W, Qing X, Jingjie W, Meng](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref20) [Y, Liang L. Low-rate DDoS attack detection](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref21) [based on factorization machine in software defined network. IEEE Access 2020;8:](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref21) [17404–18.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref21)

[22] [Verma P,](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref21) [Tapaswi S, Godfrey WW. An adaptive threshold-based attribute selection](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref22) [to classify requests under DDoS attack in cloud-based systems. Arabian J Sci Eng](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref22) [2020;45(4):2813–34.](http://refhub.elsevier.com/S2590-0056(23)00041-3/sref22)

10