International Journal on Science and Technology (IJSAT)

E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

DDoS Detection on IoT Devices Using Machine Learning Techniques

Mrs. K. Gowri[1], J. Enisha[2], P. Harini[3], M. Praveen Kumar[4]

[1]Assistant Professor, [2, 3, 4]Student
[1, 2, 3, 4]Department of Computer Science with Cognitive Systems
Sri Ramakrishna College of Arts and Science, Tamil Nadu, India

Abstract

With the emergence of technology, the usage of IoT (Internet of Things) devices is said to be increasing in people's lives. Such devices can benefit the average individual, who does not necessarily have to have technical knowledge. The IoT can be found in home security and alarm systems, smart fridges, smart televisions, and more. Although small Internet-connected devices have numerous benefits and can help enhance people's efficiency, they also can pose a security threat. Malicious actors often attempt to find new ways to exploit and utilize certain resources, and IoT devices are a perfect candidate for such exploitation due to the huge volume of active devices. This is particularly true for Distributed Denial of Service (DDoS) attacks, which involve the exploitation of a massive number of devices, such as IoT devices, to act as bots and send fraudulent requests to services, thus obstructing them. To identify and detect whether such attacks have occurred or not in a network, there must be a reliable mechanism of detection based on adequate techniques. The most common technique for this purpose is artificial intelligence, which involves the use of Machine Learning (ML) and Deep Learning (DL) to help identify cyberattacks. ML models involve algorithms that use structured data to learn from, predict outcomes from, and identify patterns. The goal of this paper is to review selected studies and publications relevant to the topic of DDoS detection in IoT-based networks using machine-learning-relevant publications. It offers a wealth of references for academics looking to define or expand the scope of their research in this area.

Keywords: DDoS Attack, Machine Learning, ANN, XGBoost, AdaBoost, SVM, Random Forest

1. INTRODUCTION

Internet of Things (IoT) was a revolutionary technology

And had become more and more beneficial in recent years. In today's world, IoT plays a crucial role in our lives. It is being used in almost every existing field like smart homes, smart cities, smart grids, autonomous vehicles, hospitals, manufacturing plants, etc. The main goal of IoT technology is to make human life more manageable and smarter by merging physical devices and digital intelligence [1] IoT devices can gather data and share them from anywhere and at any time with the help of the Internet. These data are being proceeded and analyzed inside an integrated platform and will be accessible for other IoT devices. It is estimated thattherearapprox.10.07billionIoTdevicesconnectedvia the Internet in 2021, and this number will reach 24.1 billion by 2030 [2]. Therefore, a large amount of data is being transferred between these interconnected devices, and it is essential to maintain this flow of data and protect it from cyber-attacks[1].

The security threats to IoT devices and networks can be sorted into six different categories: Denial of Service (DoS), Bogus Information, Eavesdropping, Impersonate, Hardware Tempering, and Message Suspension [2]. Among all the threats, DoS and Distributed DoS (DDoS) attacks, which are the more advanced version of Dos and they are more complicated to detect or mitigate, are the most dangerous and destructive method to take over IoT. In this type of attack, the attacker's purpose is to encumbrance the service by transmitting large volumes of data traffics, hence the service provider can't handle it, and legitimate users and devices will face problems with receiving services due to engendered disturbance [3]. There are different types of DDoS attacks with different characteristics and features. The most known types of DDoS attacks are TCP Flood, SYN Flood, UDP Flood, ICMP Flood, HTTP Flood, Ping of Death, NTP Amplification, DNS Flood, and Zero-Day DDoS [4].

The architecture of our study is shown in figure 1, and the main contributions of this study are as follows:

- Providing a novel approach to feature selection and dimension reduction on the CICDDoS2019 Dataset.
- Proposing a detection model that classifies DDoS attacks more accurately and faster compared to current state-of-the-art models.
- Specifying the most proper machine learning algorithm for DoS/DDoS detection in terms of effectiveness and efficiency by examining them inside the model.
- Determining the essential features of the CICDDoS2019 Dataset that have the highest impact on DDoS prediction.

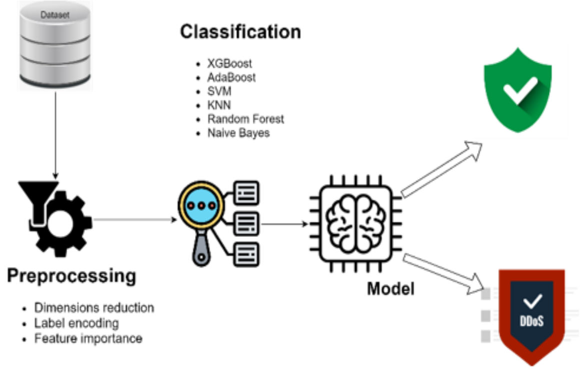

Fig. 1. The architecture of the DDoS Detection Framework

1. BACKGROUNDAND RELATED WORKS

2.1DoS and DDoS Attacks

Traditional ML models have been widely attempted to detect network intrusions. One of the earliest study found in literature that employed Bayesian algorithm as classifier, which has advantages of simplicity, easy to implement, and applicability to binary and multi-class classification [5]. Knearest neighbor algorithm was also applied for detecting DDoS attack in wireless sensor network, but it is difficult to determine the optimal K value for large datasets. Ambusaidi et al. [6] employed SVM model and developed a mutual information-based feature selection algorithm to improve the detection performance. However, with the size and dimension of thedataset increase, the accuracy of the classifier will decrease. Doshi et al. [7] tested five different ML detection methods on a dataset of normal and DDoS attack traffic collected from an experimental IoT-based network. Because traditional ML schemes heavily depend on feature engineering, it is often time-consuming and complex to calculate the correlation between features. Overall, it is impractical to detect attacks by applying traditional ML algorithms in real-time applications. The most known kinds of DoS/DDoS attacks are explained in the following paragraph.

- TCP Flood: In this type of attack, the attacker exploits a part of TCP's three-way handshake to consume target resources and render it unresponsive[8].
- SYN Flood: In an SYN Flood attack, the attacker sends consecutive SYN packets to every target's port, using a fake IP address.
- UDP Flood: This is a DoS attack in which an attacker selects random target ports and then overwhelms them with IP packets containing UDP data diagrams.
- ICMP Flood: Internet Control Message Protocol or ICMP Flood, also known as Ping Flood, is a type of DoS attack in which the attacker attempts to make the target out of reach of normal traffic by flooding the targeted device with ICMP echo-requests.
- HTTP Flood: In this type of attack, the attacker overwhelms the targeted server by sending HTTP POST or GET requests.
- Ping of Death: In this type of attack, the attacker uses simple ping command to destabilize, crash or freeze the targeted devices by sending malformed or oversized packets.
- NTP Amplification: In this type of DDoS attack, the attacker exploits Network Time Protocol (NTP) servers which are publicly accessible, to overwhelm the target with UDP traffic.
- DNS Flood: Domain Name System or DNS Flood is a type of DDoS attack in which the attacker floods one or more particular domain's DNS servers to hamper the DNS resolution of the resource records of that domain.

2.2Machine Learning Classifiers for DDoS Detection

There are various techniques for DDoS detection. However, traditional ones are becoming obsolete due to the new complicated attack types. Using data mining and machine learning techniques is the most efficient way to detect DDoS attacks and recently attracted the attention of researchers. In these kinds of techniques, a dataset is gathered from a simulation or real attack environment; then, the researchers try to extract the operative features from raw data. Subsequently, the researchers use the machine learning algorithms to train a detection model, and after that, they evaluate the performance of their model to determine whether their detection model is qualified for DDoS detection or not. A list of common machine learning algorithms for DDoS detection is available in the following paragraph.

In this subsection, a few supervised ML algorithms will be discussed. Decision tree, random forest, K-nearest neighbors, XGBoost, artificial neural networks, support vector machines, and adaptive boosting are discussed here, each with an informative brief. All these algorithms are considered within the top and most common ML model.

- ***Decision Tree (DT)***

DT is a hierarchical structure supervised algorithm in which the internal nodes represent the features of the dataset, the branches represent the decision rules, and the leaf nodes represent the outcome. The structure is illustrated in Figure 2. It classifies the instances beginning with the root downward up to the leaf nodes of the tree. DT deals with data inconsistency since all entities in a class have equivalent conditional probability values and fewer data cleansing requirements than other methods. The logic of DT can be easily understood and can mimic human thinking in decision-making [9].

- ***Random Forest (RF)***

RF is an ensemble-based supervised learning technique that merges multiple classifiers to tackle a challenging problem and improves the performance of models. RF takes less training time and maintains a high prediction accuracy even for large datasets and large missing proportions of the data [10]. Figure 4 illustrates the breakdown of RF that contains multiple decision trees for each subset of a dataset. To improve its predictive accuracy, RF aggregates the prediction outcomes of each tree to predict the outcome based on the most votes. Furthermore, to predict an accurate result, there must be some actual values in the dataset's feature variable, as well as a greater number of trees.

- ***K-Nearest Neighbors (KNN)***

KNN is a supervised, straightforward machine learning algorithm. KNN does not learn immediately from the training dataset. On the contrary, it works by storing the dataset and assuming the similarity between new and existing cases, then placing the newly identified case in the category that is most similar to the existing ones. KNN is resistant to noisy training data. However, it entails a high computational cost, as it makes its prediction based on a distance calculation using an enhanced distance algorithm [11].

- ***XGBoost (eXtreme Gradient Boosting)***

XGBoost is a gradient-boosted tree-structured implementation based on sequential enabling. Gradient descent refers to the underlying objective function; it provides substantial flexibility while delivering the desired results using computational power optimally. XGBoost can handle sparse data, parallel processing, and built-in cross-validation to reduce overfitting [12].

- ***Artificial Neural Network (ANN)***

ANN, or neural network (NN), architectures mimic the network of neurons and are derived from biological NNs that build the structure of the human brain so that computers may grasp things and make choices in a human-like manner. As depicted in Figure 5, ANNs comprise three layers: input, hidden, and output layers. The hidden layer lies between the input and output layers and can perform all the necessary calculations to find hidden patterns and features. A few advantages of ANNs are that they have a parallel processing capability, work with incomplete knowledge, and have fault tolerance. On the other hand, ANNs have hardware dependence and require assurance that the network is appropriately structured [13].

- ***Support Vector Machine (SVM)***

A SVM is a supervised learning algorithm that is widely used for classification. The SVM algorithm attempts to locate a decision boundary that differentiates the two classes in the SVM, which is also known as a hyperplane, in an N-dimensional space for each distinct dimension (with N being the number of features). SVM memory is efficient, as it utilizes a subset of the support vectors, which are the training points of the decision function. As depicted in Figure SVMs can be of two types: linear SVMs and non-linear SVMs [14]:

(A) Linear SVM: This is utilized for linearly separable data, which implies that if a dataset using a single straight line can be classified into two classes that are linearly separable, the classifier employed is called a linear SVM.

(B) Non-linear SVM: This is utilized for non-linearly separable data, which implies that if a dataset utilizing one straight line cannot be categorized, it is called non-linear data, while the classifier employed is called a non-linear SVM.

- ***Adaptive Boosting (AdaBoost)***

AdaBoost is a supervised learning boosting technique based on the ensemble iterative method. It combines multiple low-accuracy classifiers to build a single highly accurate classifier. The objective of AdaBoost is to train the data sample and set the classifier weights in each iteration to produce accurate predictions of anomalous observations. AdaBoost repeatedly adjusts the errors of the weak classifier. However, it is highly affected by noisy data [15].

3. METHODOLOGY

3.1 Proposed Study

First of all, we reviewed the related works of other researchers to determine the most common machine learning algorithms used for detecting Dos/DDoS attacks. Then we proposed a model to compare these algorithms in terms of effectiveness and speed. Next, we used the latest available Dataset, “CICDDoS2019”, as an input. After preprocessing the data, we tested the most popular machine learning algorithms and captured the data results. Finally, we specified the most important features of the “CICDDoS2019” Dataset that have the highest impact on DDoS prediction for the first time.

3.2 Dataset

In this study, we used the “CICDDoS2019” Dataset, which is the latest available Dataset in the context of DDoS attacks and has improved most of the shortcomings of the previous Dataset. This Dataset contains both Reflection-based and Exploitation-based DDoS attacks using TCP/UDP-based protocols at the application layer. The main benefit of using this Dataset is that it has proposed a new taxonomy, including new attack types. As a result, there are different categories of DDoS attack types which are labelled as 'PortMap,' 'NetBIOS,' 'LDAP,' 'MSSQL,' 'UDP,' 'UDP-Lag,' 'NTP,' 'DNS,' 'SNMP,' 'SSDP,' 'WebDDoS' and 'TFTP' and normal traffic which is labeled as 'BENIGN.' Network traffic data with their respective labels and traffic features which are extracted by CICFlowMeter-V3, are saved in a CSV file and available for free.

3.3Machine Learning Algorithms

We reviewed related works to determine machine learning algorithms used for DDoS attack detection by other researchers. Naïve Bayes, SVM, KNN, Random Forest, XGBoost, and AdaBoost were the most used algorithms in the literature, and these algorithms submitted great performance in DDoS detection experiments. We used these algorithms in our experimental model and then evaluated them to specify the best ones. In the following sections, the evaluation metrics and the results will be explained.

3.4Evaluation Metrics

For comparing experimented algorithms, we used Accuracy Score, F1-Score, ROC Curve, and Training Time, and for specifying the most important features, we used Feature Importance.

• Accuracy Score measures the ratio of true predicted labels to a total number of labels. Since our Dataset might be unbalanced, just using Accuracy Score is not a good choice. The formula of Accuracy Score is mentioned below:

$$Accuracy = \frac{(\mathrm{TP} + \mathrm{TN})}{(\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN})}$$

• F1-Score measures the harmonic average of Precision and Recall. It is a suitable evaluating metric to be accompanied by the Accuracy Score as it considers False Positive and False Negative. Formulas of Precision, Recall, and F1-Score, are mentioned in the following:

$$Precision = \frac{\mathrm{TP}}{(\mathrm{TP} + \mathrm{FP})}$$

$$Recall = \frac{\mathrm{TP}}{(\mathrm{TP} + \mathrm{FN})}$$

$$F1\ Score = \frac{2 * \mathrm{Precision} * \mathrm{Recall}}{(precision + recall)}$$

- ROC Curve or Receiver Operating Characteristic Curve evaluates the model performance by considering False Positive and False Negative Rates.
- Training Time is a metric to determine the speed and agility of the model.
- Feature Importance calculates a correlation between each feature with the predicted label.

4. RESULTS AND ANALYSIS

This section shows the result of the comparison between selected algorithms on our experimental model and CICDDoS2019 Dataset and analyses the results. As you can see in table I and figure 2, SVM, and Random Forest are the most accurate algorithms with an accuracy of 100% and an F1-Score of 1. SVM also recorded a slightly better Training Time than Decision Tree,AdaBoost. XGboost, KNN, and ANN also had acceptable accuracy of 98.5%, 98.75%, and 99.00%, and F1-Scores of 0.9850, 0.9875, and 0.9306, respectively. In our experiment, unlike previous researches, ANN and Naïve Bayes recorded an F1-Score of 0.7098, 0.7134 despite an Accuracy of 96.21%, 95.67%which is not acceptable. Therefore, it doesn't seem to be a good algorithm for DDoS detection. Furthermore, Naïve Bayes has a high False Positive Rate, which means that this algorithm classifies BENIGN traffic as ATTACK traffic wrongly. The reason that Naïve Bayes recorded a high Accuracy Score is that the Dataset is unbalanced and the number of Attack records is extremely more than the number of Benign records; thus, the number of False Positive classifications are not shown up in this metric, but we can understand this from F1-Score and Recall metrics. As we have seen, all selected machine learning algorithms except Naïve Bayes performed well in terms of efficiency and effectiveness. The main reason that ANN and Naïve Bayes didn't have acceptable performance was that this algorithm is based on Bayes Theorem, which assumes the feature as being independent and, in our Dataset, features were not wholly independent.

Table 1: Evaluation Results

Algorithms	**Evaluation Method**	
	Accuracy	**F1-Score**
Decision Tree	98.50%	0.985
Random Forest	100%	1
K-Nearest Neighbors	98.75%	0.9875
XGBoost	99%	0.9363
Artificial Neural Network	96.21%	0.7098
Support Vector Machine	100%	1
Naïve Bayes	95.67%	0.7134

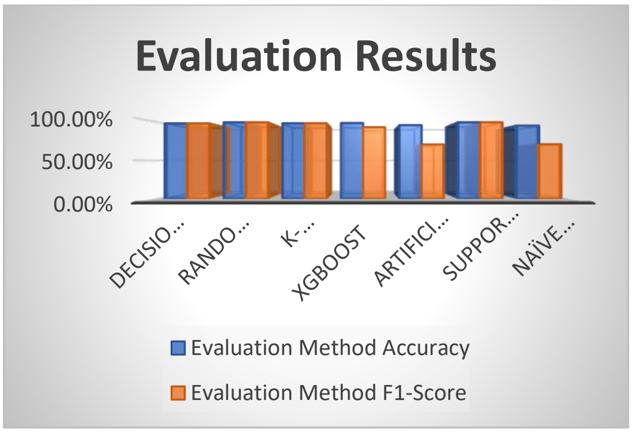

Fig 2: DDoS Detection Results

5. CONCLUSION

This paper has proposed a DDoS detection model and implemented the most popular machine learning algorithms such as ANN,Naïve Bayes, SVM, AdaBoost, XGBoost, KNN, and Random Forest, for binary classification of CICDDoS2019 network traffic into `Benign` and `Attack` classes. All of the experimented algorithms, except the Naïve Bayes algorithm, efficiently classified network traffic to Benign and Attack classes. Random Forest and SVM were extremely accurate, with an Accuracy Score of 100% and F1-Score of 1. SVM also provides slightly better training and detection time than AdaBoost. This study also specifies the top 10 most important features for DDoS detection, which have the highest impact on successful prediction. This is a substantial work since selecting the most pivotal features and removing nonsignificant ones would help the detection model to be trained better and have higher accuracy and speed and also would prevent the overfitting of the model.

References:

[1] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," IEEE Access, vol. 9, pp. 42236-42264, 2021.

[2] N. Jyoti and S. Behal, "A Meta-evaluation of Machine Learning Techniques for Detection of DDoS Attacks."

[3] S. Mishra, C. Mahanty, S. Dash, and B. K. Mishra, "Implementation of bfs-nb hybrid model in intrusion detection system," in Recent Developments in Machine Learning and Data Analytics. Springer, 2019.

[4] D. Papamartzivanos, F. G. Marmol, and G. Kambourakis, "Dendron: ´ Genetic trees driven rule induction for network intrusion detection systems," Future Generation Computer Systems, vol. 79, pp. 558–574, 2018.

[5] T. Kawamura, M. Fukushi, Y. Hirano, Y. Fujita and Y. Hamamoto, "An NTP-based detection module for DDoS attacks on IoT", 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2017

[6] W. N. H. Ibrahim et al., "Multilayer framework for botnet detection using machine learning algorithms," IEEE Access, vol. 9, pp. 48753- 48768, 2021.

[7] Amrish, R.; Bavapriyan, K.; Gopinaath, V.; Jawahar, A.; Vinoth, C.K. DDoS Detection using Machine Learning Techniques. J. IoT Soc. Mob. Anal. Cloud 2022, 4, 24–32.

[8] A. Rezaei, "Using Ensemble Learning Technique for Detecting Botnet on IoT," SN Computer Science, vol. 2, no. 3, pp. 1-14, 2021.

[9] Alkasassbeh, M.; Al-Naymat, G.; Hassanat, A.B.; Almseidin, M. Detecting Distributed Denial of Service Attacks Using Data Mining Techniques. Int. J. Adv. Comput. Sci. Appl. (IJACSA) 2016.

[10] S. Wankhede and D. Kshirsagar, "DoS attack detection using machine learning and neural network," in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018: IEE.

[11] K. S. Hoon, K. C. Yeo, S. Azam, B. Shunmugam, and F. De Boer, "Critical review of machine learning approaches to apply big data analytics in DDoS forensics," in 2018 International Conference on Computer Communication and Informatics (ICCCI), 2018: IEEE.

[12] Roopak, M.; Tian, G.Y.; Chambers, J. An Intrusion Detection System Against DDoS Attacks in IoT Networks. In Proceedings of the 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020.

[13] Prasad, A.; Chandra, S. VMFCVD: An Optimized Framework to Combat Volumetric DDoS Attacks using Machine Learning. Arab. J. Sci. Eng. 2022.

[14] Sharma, D.K.; Dhankha, T.; Agrawal, G.; Singh, S.K.; Gupta, D.; Nebhen, J.; Razzak, I. Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks. Ad Hoc Netw. 2021.

[15] Hassan, K.F.; Manna, M.E. Detection and mitigation of DDoS attacks in the Internet of things using a fog computing hybrid approach. Bull. Electr. Eng. Inform. 2022.