EFFICIENT CLASSIFIER TO DETECT DDoS ATTACK BASED ON INTERNET OF THINGS

by

Fatimah ALMULHIM[a], Huda M. AL SHANBARI[a], Hassan M. ALJOHANI[b], Azhari A. ELHAG[b], and Anis Ben ISHAK[c,d*]

[a] Department of Mathematical Sciences, College of Science,
Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia
[b] Department of Mathematics and Statistics, College of Science, Taif University, Taif, Saudi Arabia
[c] Department of Quantitative Methods, Higher Institute of Management,
University of Tunis, Tunis, Tunisia
[d] University of Manouba, ESCT, QuAnLab LR24ES21, Campus Universitaire, Manouba, Tunisia

Original scientific paper
https://doi.org/10.2298/TSCI2406113A

An intriguing mechanism that facilitates easy connection between several devices is the internet of things (IoT). This encourages the creation of fresh methods for automatically detecting client IoT occurrence traffic. Through this study, we show that several kinds of machine learning methods may produce great accurateness distributed denial of service (DDoS) detection in IoT network traffic by exploiting IoT-particular network characteristics to guide choice of features. The results of the study demonstrated that our system detected DDoS attacks with high precision, confirming its dependability and robustness in IoT network. A DDoS detection algorithm that utilizes machine learning approaches is proposed in the present study. The most recent dataset, CICDDoS2019, was utilized to write this research. It tested a variety of well-liked machine learning techniques and identified the attributes that most closely correspond with projected classes. It is found that random forest was 99.5% accurate in predicting the type of network procedure, demonstrating their extraordinary accuracy.

Key words: *cyber attack, DoS, DDoS, machine learning, random forest*

Introduction

Technology is advancing quickly, devices are getting cheaper and more compact, and it is adapting to the present ever-connected connections. This renaissance makes it easy for any device to interact and develop the online world of the future. The IoT, a *paradigm-shifting*, impending model in the field of cellular connectivity, along is acknowledged as the new idea of the worldwide web the future [1].

The IoT can be summed up as an internet of interconnected things, which includes things like sensors, mobile phones, digital technology, RIFD (radio frequency identification tags), as well as individuals who are assigned unique identifiers (UID) and are able to interact over a connection lacking the use of a machine [2]. The IoT implementations have a wide range of constantly expanding uses. Public security, development in infrastructure, linked medical care mechanisms, smart cities, smart homes, smart grids, wearable technology, mechanization in industry, commercial facility*, etc.* are just a few of the applications that heavily rely on

* Corresponding author, e-mail: anis_isg@yahoo.fr

the IoT [3]. A variety of threats could try gain access over the entire network or prevent the IoT from providing its services. However, DDoS assaults position the utmost threat to an IoT system. When a DDoS assault is distributed, it means that it is carried out on the internet by several hackers or proxies operating from different places [4]. There will be a finite number of resources available to any connected device. A network that is subjected to a *denial-of-service* attack will begin allocating its resources to fulfill the demands. Yet, a network will stop serving requests whenever the volume of requests exceeds what it can process. Any demand, even from authorized users, would be turned down, which would interfere with the provision of the services by IoT [5].

Through the aid of the world wide web, IoT gadgets may gather and distribute data at several times and from whichever location. Other IoT's gadgets will be able to access and use this data as they are processed and evaluated inside a single system. It is projected that by 2030, there will be 24.1 billion internet-connected objects worldwide, up from an expected 10.07 billion in [6]. As a result, a lot of data is being exchanged back and forth across these networked devices, and it is crucial to keep this data flowing and safeguard it against intrusions [7]. Six groups can be used to group security risks to IoT networks and equipment: communication being suspended, hardware tampering, impersonation, eavesdropping, DoS, and false data [7]. The most hazardous and devastating way to take over IoT among all the dangers is through DDoS assaults, which are a more refined kind of DoS and more problematic to perceive or counter [7, 8]. The goal of this kind of occurrence is to problem the service by delivering enormous amounts of data traffic, which the service provider not able to handle. As a result, honest customers and their gadgets will experience issues obtaining provisions because of the disruption that this form of attack causes [9]. The DDoS assaults come in a assortment of forms with unique traits and attributes. The TCP Flood, SYN flood, UDP flood, ICMP flood, HTTP flood, ping of death, NTP amplification, DNS flood as well as A zero-day DDoS are the most well-known forms of DDoS attacks [10].

The IoT knowledge is attractive an essential aspect of our lives as its use expands daily. Nevertheless, as was already highlighted [10], dangers to cybersecurity, particularly DDoS assaults, are serious issues and roadblocks. Thus, in recent years, researchers have become interested in DDoS detection. The majority of the detection methods for DoS or distributed detection put out by researchers relied on artificial intelligence techniques [11].

Cyber-security in IoT

The phrase *cyber-security* is frequently used to refer to the defense of networks and systems for computers against threats involving information, programs, or infrastructure. The phrase, its meaning, and its significance have evolved over time despite many specifics being in dispute. These developments are related to the concern about how the community maintains the integrity of our informational facilities and technology, particularly the web, for the benefit of nations, groups, and society as a whole at large. When discussing cyber-security, one must consider systems that are vulnerable, such as banking networks, consumer electronics, and the IoT, as well as the possible consequences of network security incidents, data corruption or theft, and the preventative measures put in place for safeguarding them, such as routers and security procedures [12].

Cyber-attacks overview

Cyberattacks known as IoT attacks are directed at devices with internet access including printers, security cameras, and thermostats. Because these gadgets are frequently left unattended, thieves can easily access them. Attacks on the IoT can be as basic as DoS assaults or as

complex as device hijacking and using the equipment to launch additional attacks. Attacks by hackers seek to jeopardize the accessibility of data, security, and quality. Viruses, worm and the trojans, malware, denial-of-service attempts, web-based crimes, fraudulent transactions, social engineering, and stolen gadgets are a few of the more prevalent forms of cyberattacks. When it comes to safeguarding the security, reliability, or accessibility of data, intrusions are a constant worry for authorities, companies, and single people equally due to the web's ever-evolving architecture and technological advancements.

Denial-of-service attack

The goal of attacks known as denial-of-service is to prevent users from accessing a computer or network resources. Though an online attack coming from only one IP address can be stopped via an additional firewall rule, there are numerous more types of attacks that can occur, making it much harder to safeguard across them. These stabbings may originate from *zombie bot computers*. An substitute technique entails trapping naive systems-dubbed *botnets* from the term *robot* – into transmitting traffic towards the intended target.

Distributed denial of service attack works

Among the main threats to the security of IoT networks is DDoS assaults. Several compromised nodes are used by the hacker in the current attack to take over the victim by generating a large amount of network traffic that utilizes up the destination's bandwidth. In the end, this results in the destruction of the infrastructure, disruptions to services, and blocking of related services from those with permission. The DDoS assaults use two different kinds of methods: amplified and reflections. The aggressor utilizes the target's IP address as the containers' originating address and the reflection technique to deliver packets to many destinations. However, the assailant sends a lot of packets to the target's system by using the amplified approach [13]. There are several ways to execute DDoS assaults, which are enumerated:

- The TCP Flood: This kind of attack uses a flaw in TCP's three-way handshake to overwhelm the victim's capacity and cause it to become unresponsive [14].
- The SYN Flood: Using a invented IP address, the intruder sends a sequence of SYN packets to every target's port.
- The UDP Flood: This category of denial-of-service attack involves picking arbitrary object ports and flooding them using IP packets which include UDP data diagrams.
- The ICMP flood: *Internet Control Message Protocol*, sometimes referred to as ping flood, is a kind of denial-of-service assault in which the assailant bombards the victim's computer with ICMP echo messages in an effort to render it unreachable by regular traffic.
- The HTTP Flood: In this kind of threat, a large number of HTTP POST or GET requests are sent towards the target's location by the intruder.

To be able to decrease and avoid DoS stabbings, it is imperative to comprehend their many sorts and tactics that aim at securing up a targeted server, which could potentially be an IoT device. The IoT networks may potentially be theme to a variability of DoS attacks, including the smurf and SYN flood assaults [15]. Using a fake IP address, a Smurf threat bombards the directed server with internet control message protocol (ICMP) requests. The communication request's status, including the probability that it reaches its destination, is to be reported to the sender by the ICMP. Networking equipment like the routers use ICMP. A Smurf attack operates on the following principle: the intruder sets the original IP address of the spoof traffic to that of the target server, and then sends it via a router's IP broadcasting addressing. Subsequently, the fake ip of the object being targeted receives queries from the routers, and the host

devices within the system reply through sending ICMP packets to that address. As a result, the target server will receive an excessive number of queries [16]. However, since the intruder actually establishes a joining after demanding the server, the SYN flood is observed as a half-open assault. As a result, its goal is to establish a TCP session. To keep the data sequence among the person who sends it and the recipient, TCP and IP operate in tandem. To establish the connection during the handshake phase, an individual sends a SYN container to the recipient. In reply, it sends a reply (ACK) and waits for the sender to send another ACK. When an attacker sends a fake message without providing an additional ACK in response, the computer will respond with an ACK in the SYN flood attack. Until every port on the server is being used, the attacker will keep transmitting SYN packets to the server [17]. The SYN flood risk is the most common sort of DoS harm, and the transmission control protocol (TCP) is used in almost all (85%) of DoS attacks, based on [14].

Related work

Ates *et al*. [16] proposed a DDoS detection approach based on the relationships between request packet information. They utilized the SVM technique, the principles of entropy and modularity, and both real-world extracted data and the Caida dataset in their studies. Their findings revealed that applying modularity concepts in TCP connections and randomness in UDP communications resulted in higher detection accuracy. Ibrahim *et al*. [17] introduced a tiered architecture employing machine learning techniques to identify botnets facilitating DDoS attacks. Using a novel method for feature extraction, classification, and hyperparameter tuning, they evaluated KNN, SVM, and MLP methods within their proposed architecture on the CTU-13 dataset. Contrary to prior research findings, they observed that the use of oversampling strategies did not enhance the accuracy of the models. Within the structure that they suggested, the KNN algorithm achieved the utmost correctness of 91.51%. Based on seven variables taken from user discussions, She *et al*. [18] created a model to differentiate between botnets, which are used to launch DDoS assaults on the application layer, and ordinary users. Utilizing a single-class SVM technique on their collected dataset, they deduced that their algorithm was fruitful in sensing DDoS attacks at the application layer. An machine learning algorithm was published by Amrish *et al*. [19] to classify both normal and DDoS packets to identify whichever model of classification was most effective at identifying illegal IP addresses. The CICDDoS2019 dataset was utilized for learning and evaluate classification classifiers. The best fifteen characteristics have been selected from this dataset, which consists of several DDoS attack occurrences with one class variable and 88 attributes. Four algorithms were used to assess this work: ANN, KNN, RF, and DT. The ANN was found to be the greatest accomplishment model, with a 99.95% efficiency rating. False negatives were more frequent than false positives, which were absent. In order to provide a machine learning based technique for identifying DDoS-infested traffic in consumer IoT (CIoT), Gupta *et al*. [20] examined characteristics of connected devices. According to this study, there are several basic differences between the flow of traffic of typical internet-connected devices and those of IoT sensors. In order to collect regular and malicious traffic movements and produce a dataset, the authors replicated an IoT network. Six machine learning models – the NB, DT, SVM, RF, KNN, and logistics regression (LR) algorithms – were employed for detecting based on the acquired dataset. The local router blocked malicious traffic as an extra mitigation measure. The findings from experiments have an accuracy between 0.97 and 0.99. But when it came to assault detection, RF was the classification that performed the best and was also most precise and trustworthy. It received 0.967 for the performance factor of precision, 0.989 for performance factor of recall, and 0.97 for

performance factor of F-measure. Furthermore, it produced minimal false alarms, as seen by its low false-positive percentage of 0.008.

Methodology

Machine learning models for DDoS detection

The machine learning is a technology that enables processors to mechanically acquire from historical statistics and make choices similar to those made by people. In machine learning, a model is trained using data from training, and then new data is processed to produce a forecast, recognition, or classifier. Network security is starting to use this knowledgeable approach, which solves the drawbacks of less intelligent methods. Additionally, networks are able to be shielded from intrusions by using machine learning or deep learning techniques that are trained using network information differentiate between benign and dangerous connections. Furthermore, the algorithms can be learned to recognize the sort of attack and conduct the appropriate countermeasures if the internet activity is fraudulent. The present research focuses on these applications of smart approaches, which may prove advantageous in various scenarios.

Decision tree

The inner nodes of decision tree (DT), which is an organized supervised method, stand in for the dataset's features, the branching for the selection rules, and the nodes on the leaf for the result. Unlike other approaches, DT requires less data purification while all entities within a class have similar conditionally probable values. This helps it deal with inconsistent data. DT's reasoning is simple to comprehend and may be employed to simulate how people make decisions [21].

The K-nearest neighbors

A simple, supervised machine learning method is K-nearest neighbors (KNN). It takes some time to learn using the materials used for training. Instead, it stores the dataset, makes an assumption about the resemblance between novel and prevailing cases, and then assigns the recently discovered case into the group of cases that shares the greatest similarities with the previous examples. Noisy training data does not affect KNN. Nevertheless, because it bases its predictions on an actual distance measurement utilizing an improved distance method, it has a high processing cost [22].

The XGBoost (eXtreme gradient boosting)

The XGBoost is a sequentially enabled gradient-boosted tree-structured solution. The fundamental objective of this variable is known as slope descent, and it offers significant adaptability while maximizing the use of processing capacity to get the intended outcomes. Sparse facts, processing in parallel, and integrated cross-validations to lessen excessive fitting are all supported by the XGBoost [23].

Adaptive boosting

Adaptive boosting (AdaBoost) is an aggregation iteration method-based supervised learning boosting strategy. It creates a single, highly precise classification by combining several low accuracy classifications. In order to generate accurate forecasts of unusual findings, AdaBoost goals to train the data samples and established its classification parameters in each reiteration. AdaBoost is continuously modifies the weak classifier's mistakes. Yet, data that is noisy has a significant impact on it.

Support vector machine

A prevalent supervised learning procedure for classification is the support vector machine (SVM). For every individual degree, the SVM algorithm looks for a decision boundary, also called a hyperplane, in a space with N dimensions that distinguishes between the two subclasses in the SVM. Because it uses a portion of the support vectors – the decision function's learning points – SVM storage is effective.

Random forest algorithm

To find out whatever machine learning techniques earlier investigators have employed for DDoS attack identification, we examined related literature. The most popular algorithms in research were Naive Bayes, SVM, KNN, random forest (RF), XGBoost, and AdaBoost. These algorithms demonstrated excellent performance in DDoS recognition tests. The aforementioned procedures were employed in our research model, and the optimal ones were determined via evaluation. Using personal datasets, we examined multiple articles on machine learning approaches that were applied to develop or contrast models with the purpose of identifying and categorizing DDoS attacks. The method that we have used for DDoS attack detection is called RF. The RF is a technique for combined learning that is created by merging numerous DT models. Every DT in RF is created on their own using various sample sizes and subsections of features as the foundation for the creation method. The fundamental idea behind RF is to build numerous DT in order to decrease the likelihood of overfitting a single DT and increase the model's ability for generalizations. A part of the initial information that is aimlessly nominated is used to train each DT in RF. By polling or averaging the consequences of every DT, RF carries out regression or classification [24-30]. There are numerous essential variables in the RF. The sampling rate, the number of DT, and the number of attributes in every DT are the three most crucial among these variables. The precision and processing efficiency of RF can be adjusted by adjusting these variables. Numerous industries, including finance, healthcare, artificial intelligence, natural language processing, and others, have found extensive uses for radiofrequency technology. High accuracy, handling a huge number of attributes and tests, identifying significant characteristics, handling data that is missing, and other capabilities are some of its benefits. As depicted in fig. 1. The following is the RF method's core workflow.

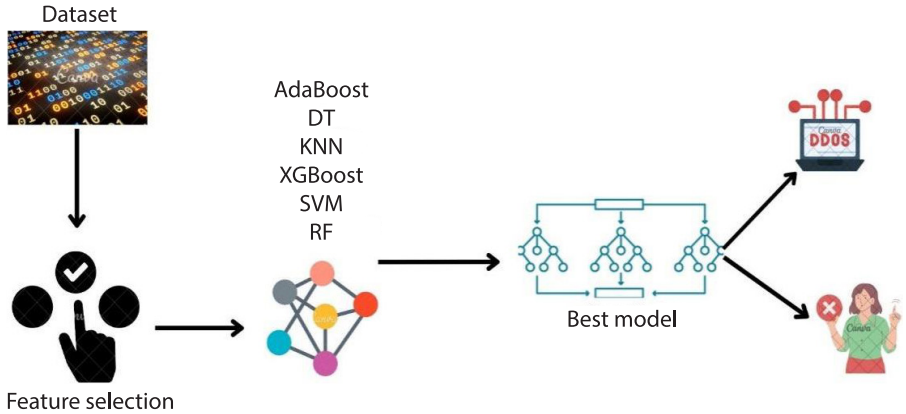

Figure 1. The DDOS Detection framework

Dataset

A publicly available dataset produced by the Canadian institute for cyber security (CIC) is called CIC-DDoS2019. Data on network traffic from DDoS attacks produced with a range of attacker tools and methodologies is included in the collection. The 53 distinct DDoS assault situations are included in the collection, each of which represents a unique set of attack tools, targets, and victim networks. A series of sensors placed on the network used by the victim captures the network traffic during the attacks, which are created in a controlled setting. Eighty million network flows – both malicious and legitimate – are included in the dataset. Eighty-eight attributes, comprising data such protocols type, payload size, time frame, and both destination and source IP addresses, are used to define each session. The goal of the CIC-DDoS2019 dataset is to support research endeavors like the creation of machine learning algorithms for DDoS defense and identification. The dataset is free to use for non-profit purposes and can be downloaded from the CIC webpage. First, we have taken 81 attributes totaling thirty thousand records from the CICDoS2019 dataset, which includes the most recent DDoS attacks. This dataset makes up for the flaws and restrictions of the preceding dataset by simulating the real data flow features as closely as feasible. Data type changes, feature encoding, default value padding, redundant information elimination, and data rebalancing were the initial pre-processing steps applied to the data set. This information must then be standardized in order to bring the values into harmony. Equations *x*, which transforms the initial data set into values in the interval [0, 1], is used for normalizing the data. Ultimately, twenty-three percent of the test set and 77% of the initial training set for predicting models were taken from the CIC-DDoS2019 dataset.

Algorithm 1: Feature Selection Algorithm
Dataset = CIC-DDoS2019
Featurealgorithm=Wrapped method,
{variance, forward feature selection,backward feature selection}
Model = RandomForest
Procedure: *FeatureSelection*
Step 1: *defined*:
featureresults = [],
featureset = [1-53],
featureset 1 = *[]*,
featureset 2 = [], *... FeatureSet 3 = []*,
Step 2: f*or each featureAlgorithm in featureAlgorithms*:
feature Set 1 = variance(datasets),
feature Set 1= forward feature selection(datasets),
feature Set 1 = backward feature selection(datasets),
Step 3 : *for each featureNums in featureSet*:
Condition-if featureNums ≥ 0 then:
add featureNums.index in featureResults
Step 4: *return featureResults*
endprocedure

Evaluation indicators

Three metrics are used to assess the effectiveness of detection of intrusions techniques: accuracy (AUC), the *rate of true positives* (TPPR), and the *rate of false positives* (FPR). High TPR, low FPR, and high *A***O**C are the characteristics of a good detection method. The review of the measures and the findings will be described for each of the parts that follow.

FPR is the lowest grade classification rate, accuracy, TPR, and TPR increase the high quality classification ratio.

Accuracy-the ratio of true predicted labels to all labels is measured by the accuracy score. It is not an effective strategy to rely solely on efficiency score because our dataset might not be properly equal. The following is the formula for scoring accuracy:

$$ACC = \frac{Tp + Tn}{Tp + Fp + Tn + Fn} \tag{1}$$

The TPR-naturally, the true positive rate expresses the proportion of positive data points associated with all positive information units that are appropriately interpreted as positive. In alternative reasoning, when the TPR increases, we will mistake fewer positives' data points:

$$TPR = \frac{Tp}{Tp + Fn} \tag{2}$$

The FPR-the number of findings that are forecasted as positive out of all the negative cases is known as the false positive rate. Put otherwise, the number of negative cases that are mistakenly classified as positive:

$$FPR = \frac{Fp}{Tn + Fp} \tag{3}$$

When an attack's data that is appropriately categorized as anomalous is represented by TP. When data is appropriately identified as normal, it is represented as TN. The FP The stands for legitimate data that is mistakenly labeled as an intrusion; on the other hand, FN denotes data that is unusual that has been mistakenly labeled as usual.

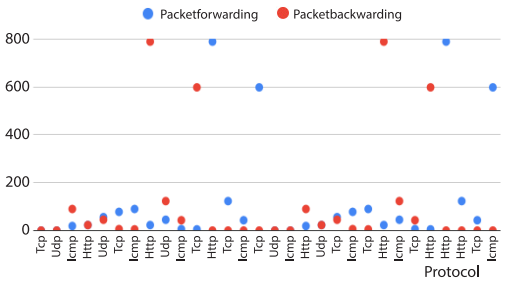

Figure 2. Comparison of packet forwarding and packet back warding in TCP, UDP, ICMP, and HTTP protocols

Experiment results

Assessment of packet forwarding and packet back warding

In fig. 2. packet backward alerts the originator when traffic in the opposing path of the received warning necessitates the initiation of congestion avoidance actions. It means that there's a chance that the user's packets on this logical connection will run into resource congestion. Packet forwarding alerts the user when traffic in the same route as the incoming warning requires the initiation of congestion-avoiding operations. It means that the packet in question has run into capacity congestion in the several protocols on this logical link.

Assessment of DDoS attack detection in TCP, UDP and other protocols

In fig. 3. by using a reputable third-party element, the attacker's identification during a DDoS attack is kept secret. Hackers send packets to reflective systems with the original IP address configured to the IP domain of the intended victim in an attempt to overwhelm the victim with reply packets. Such attacks can also be executed via transport layer protocols, like TCP and UDP, applied to the application layer. The SYN flood is one type of TCP-based ex-

ploited attack, whereas UDP-based attacks including UDP-Lag and UDP-Flush. Submitting a big quantity of UDP data packets to the target computer starts a UDP flood assault.

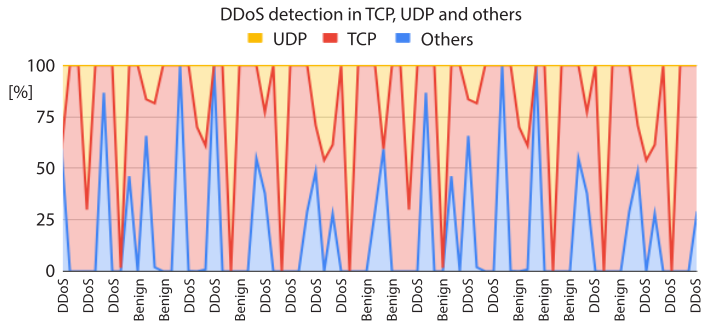

Figure 3. Assessment of DDoS attack detection in TCP, UDP and other protocols

Assessment of different detection algorithms

In the testing state, we use the conventional Decision tree, KNN, XGBoost, AdaBoost, SVM, and RF model, algorithms to perform independent tests for IoT detection of intrusions, tab. 1. demonstrate how these approaches operate differently. Compared to the classic machine learning oriented methodologies and the classification RF model, the one suggested in this study is clearly superior. Particularly, the correctness of the suggested model has been unquestionably attained at 99.5% compared to the RF based method. Furthermore, compared to the remaining algorithms, the false positive rate has entirely decreased. All things considered, the recently created approach produces low FPR and high TPR without requiring a lot of running time.

Table 1. Detection performance results

Algorithms	Evaluation method		
	ACC [%]	TPR	FPR
DT	89.5	84.62	2.6
KNN	86.56	81.62	4.2
XGBoost	82.6	86.54	2.3
AdaBoost	85.78	86.53	2.4
SVM	87.98	89.23	1.9
RF	99.5	92.5	1.5

This part presents and evaluates the outcome of comparing a few chosen methods on the experimental model we constructed with the CICDDoS2019 dataset. Table 1 and the fig. 4 show that, in our study, RF is the furthermost efficient technique, with an accuracy of 99.5%, an excellent positive percentage of 92.5, and a rate of false positives that is low. It appears to be a useful technique for DDoS detection as a result. In addition, KNN incorrectly labels BENIGN traffic as ATTACK traffic due to its high false positive rate. Because the data set is uneven because there are substantially more Attack data than benign documents, KNN reported an excessive accuracy score. As a result, the quantity of false positive classifications is not displayed in this the metric system, yet we are still able to comprehend this TPR.

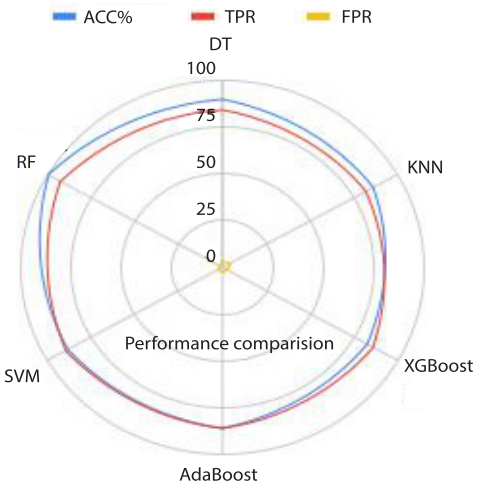

Figure 4. Detection performance results

Conclusion

In this the purpose of distinct classifying CICDDoS2019 network traffic into *benign* and *attack* categories, this study developed a DDoS finding model incorporating the most widely used machine learning algorithms, including DT, SVM, AdaBoost, XGBoost, KNN, and RF. The RF algorithm effectively categorized network traffic to benign and attack classes. With an accuracy score of 99.5%, RF outperformed rival DT, SVM, AdaBoost, XGBoost, and KNN in terms of learning and detecting time. Its strong TPR as well as low FPR further contribute to its superior precision. The contrast of packet forwarding and packet backwarding for DDoS detection in TCP, UDP, ICMP, and HTTP protocols as well as the comparison of DDoS assault detecting in TCP, UDP, and other protocol are also included in this research. These comparisons have the greatest influence on effective predictions. This is a major task because it will assist train the model for detection more effectively, increase its precision and quickness, and keep it from overfitting by identifying the most important features and eliminating those that are not crucial.

Acknowledgment

The authors extend their appreciation to the Deanship of Scientific Research and Libraries in Princess Nourah bint Abdulrahman University for funding this research work through the Research Group project, Grant No. (RG-1445-0035).

References

[1] Sadique K. M., *et al*, Towards Security on Internet of Things: Applications and Challenges in Technology, *Procedia Computer Science*, *141* (2018), Jan., pp. 199-206
[2] Al-Hadhrami, Y., *et al.*, DDoS attacks in IoT Networks: A Comprehensive Systematic Literature Revie, *World Wide Web*, *24* (2021), 3, pp. 971-1001
[3] Yousuf, O., Mir, R. N., A Survey on the Internet of Things Security, *Information and Computer Security*, *27* (2019), 2, pp. 292-323
[4] Misra, S., *e al.*, A Learning Automata-Based Solution for Preventing Distributed Denial of Service in Internet of Things, *Proceedings*, International Conference on Internet of Things, and 4th International Conference on Cyber, Physical and Social Computing EEE, Dalian, China, pp. 114-122
[5] Mirkovic, J., *et al*., A taxonomy of DDoS attack and DDoS Defense Mechanisms, *ACM SIGCOMM Computer Communication Review*, *34* (2004), 2, pp. 39-53
[6] Li, J., *et al*., The RTED-SD: A Real-Time Edge Detection Scheme for Sybil DDoS on the Inter, net of Vehicles, *IEEE Access*, *9* (2021), Jan., pp. 11296-11305
[7] Pokhrel, S., The IoT Security: Botnet Detection in IoT Using Machine Learning, *preprint arXiv*, On-line first, https://doi.org/10.48550/arXiv.2104.2231
[8] Aljuhani, A., Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments, *IEEE Access*, *9* (2021), Mar., pp. 42236-42264
[9] Jyoti, N., Behal, S. A., Meta-Evaluation of Machine Learning Techniques for Detection of DDoS Attacks, Presented, *Proceedings*, 8th Int. Conf., on Computing for Sustainable Global Development (INDIACom), IEEE, New Delhi, India, 2021
[10] Ragavendran, U., Shielding techniques for Application Layer DDoS Attack in Wireless Networks: A Methodological Review, *Wireless Personal Communications*, *120* (2021), June, pp. 2773-2799
[11] Fischer, A., *et al*., Detecting Equipment Activities by Using Machine Learning Algorithms, *IFAC-PapersOnLine*, *54* (2021), 1, pp. 799-804
[12] Makuvaza, A., *et al.*, Deep Neural Network (DNN) Solution for Real-time Detection of Distributed Denial of Service (DDoS) Attacks in Software Defined Networks (SDNs), *SN Computer Science*, *2* (2021), 2, pp. 1-10
[13] Santos, R., *et a*l., Machine Learning Algorithms to Detect DDoS attacks in SDN, *Concurrency and Computation, Practice and Experience*, *32* (2020), 16, e5402
[14] Khan, Y., *et al.*, Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications, *Electronics*, *12* (2022), 1, 88

[15] Rezaei, A., Using Ensemble Learning Technique for Detecting Botnet on IoT, *SN Computer Science*, *2* (2021), 3, pp. 1-14
[16] Ates, C., *et al*., Clustering-Based DDoS Attack Detection Using the Relationship between Packet Headers, *Proceedings*, Innovations in Intelligent Systems and Applications Conf., (ASYU), Izmir, Turkey, 2019, pp. 1-6
[17] Ibrahim, W. N. H., *et al.*, Multilayer Framework for Botnet Detection Using Machine Learning Algorithms, *IEEE Access*, *9* (2021), Feb., pp. 48753-48768
[18] She, C., *et al*., Application-layer DDoS Detection Based on a One-Class Support Vector Machine, *International Journal of Network Security and Its Applications (IJNSA)*, *9* (2017), 1, pp. 13-24
[19] Amrish, R., *et al*., The DDoS Detection Using Machine Learning Techniques, *J. IoT Soc. Mob. Anal. Cloud*, *4* (2022), Oct., pp. 24-32
[20] Gupta, B. B., *et al*., Smart Defense Against Distributed Denial of Service Attack in IoT Networks Using Supervised Learning Classifiers, *Comput. Electr. Eng.*. *98* (2022), 107726
[21] ***, Decision Tree Classification Algorithm. JavaTpoint. Available: https://www.javatpoint.com/ machine-learning-decision-tree-classification-algorithm
[22] ***, K-Nearest-Neighbor Algorithm. JavaTpoint. Available: https://www.javatpoint.com/ k-nearest-neighbor-algorithm-for-machine-learning
[23] Yiu, T., Understanding Random Forest Towards Data Science, Available Online: https://towardsdatascience.com/understanding-random-forest-58381e0602d2, 2019
[24] ***, What Is a Random Forest, Available: https://www.tibco.com/reference-center/what-is-a-random-forest xgboost
[25] Ghatak, K., XGBoost Algorithm in Machine Learning, Naukri Learning, Available Online: https://www.shiksha.com/, 2022
[26] ***, Online-courses/articles/xgboost-algorithm-in-machine-learning/ Artificial Neural Network Tutorial. Javatpoint. Available online: https://www.javatpoint.com/artificial-neural-network
[27] ***, Recurrent Neural Network Algorithms Overview. BUSINESS & AI: Artificial Intelligence for Better Decision Making, Available: https://indatalabs.com/blog/artificial-intelligence-decision-making
[28] ***, The Ultimate Guide to AdaBoost Algorithm|What Is AdaBoost Algorithm, Great Learning, Available online: https: //www.mygreatlearning.com/blog/adaboost-algorithm, 2022
[29] ***, Boosting in Machine Learning|Boosting and AdaBoost. Geeksforgeeks, Available online: https:// www.geeksforgeeks.org/ boosting-in-machine-learning-boosting-and-adaboost/, 2022
[30] Almaraz-Rivera, J. G., *et al*., Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models, *Sensors*, *22* (2022), 3367

Paper submitted: June 21, 2024
Paper revised: October 5, 2024
Paper accepted: October 28, 2024