A DDoS Attack Detection System: Applying A Hybrid Genetic Algorithm to Optimal Feature Subset Selection

1st Abid Saber
Operational Research Department
USTHB, AMCD&RO Laboratory
Bab Ezzouar, Algiers, Algeria
saberabid1@outlook.com

2rd Moncef Abbas
Operational Research Department
USTHB, AMCD&RO Laboratory
Bab Ezzouar, Algiers, Algeria
moncef_abbas@yahoo.com

3nd Belkacem Fergani
Electronics and Computer Sciences Department
USTHB, LISIC Laboratory
Bab Ezzouar, Algiers, Algeria
bfergani@gmail.com

2020 4th International Symposium on Informatics and its Applications (ISIA) | 978-1-7281-9652-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/ISIA51297.2020.9416558

***Abstract*—The rapid evolution in technology is a great challenge for network security against computer threats. Indeed, distributed denial of service (DDoS) attacks aim to deplete or even cripple target networks with malicious traffic. However, before they can be dealt with, these attacks must be identified through real-time analysis of the NetFlow sent by the routers. A large amount of flow during attacks requires the design of a standalone detector with high capacity to support this load and capable of processing traffic in real-time but with low computation time. For the same purpose, detectors based on machine learning suffer from being uncompetitive because they produce many false positives and above all require a lot of computing resources. In order to overcome these problems, in this article, we propose DDoS-Detector, a new identification and detection system, we identify the most relevant features of malicious traffic and develop a suitable concept for real-time DDoS detection.**

***Index Terms*—Distributed Denial of Service, Machine learning, Network Traffic, Hybrid Genetic Algorithm, Feature Selection.**

I. Introduction

The computer network [1] is likely to be vulnerable to attacks, which continue to multiply day by day, particularly with the increase in the number of commercial exchanges on the Internet and the development in programming techniques [7] in recent times. Additionally, a flaw in a computer system can be exploited by an attack, which is usually harmful and used for unknown purposes.

Among the most common types of computers attacks are distributed denial of service (DDoS) attacks [16]. These are attacks that aim to disrupt the proper functioning of service, to make access by legitimate users unavailable, and involve using a group of infected machines, controlled by a botnet, to send a large amount of illegitimate traffic [12] to the victim's destination. The latter, having exhausted its resources, becomes totally paralyzed and can no longer respond adequately to legitimate traffic. In addition, this attack can also induce a network overload on all network links leading to this victim, thus affecting his network operator, which will cause damage to the companies connected to this network.

Given the risk of this attack [13], and despite the continuing enthusiasm of the scientific community and the enormous costs incurred by companies to develop effective systems to counter this threat, there does not seem to be a real consensus on any detector.

An effective detector [4] is one that can both act in real-time and provide maximum information [16] about the attack in question. Indeed, we often do not find them in the literature, although recent approaches based on machine learning [14] offer better detection capabilities [11], they generate many false alarms. Moreover, they are resource-intensive as they suffer from computational complexity due to the volume of information [17] that must be processed during the training phase and also when they are deployed in production to process traffic in real-time.

Approaches that rely primarily on machine learning use their algorithms to learn the properties that characterize this type of attack to detect malicious behavior by analyzing the network traffic [15] that exploits the information from the latter. Network traffic analysis can provide an even richer perspective on the activity [19] and help identify malicious traffic and then apply the necessary security measures at the appropriate time. In the same sense, a good detection system must be able to continuously adapt to changing attack behavior over time. Indeed, rapid adaptation to changes in attack behavior over time is essential [16].

An analyzer can generate a lot of information from the flow [7], there are two main types of flow analyzers: Non-commercial and/or free operating system based and designed for small or medium-size networks, such as Nfsen, nfdump. On the other part, we have the Commercial and/or fee-based are based on proprietary systems and are very competent and flexible but are very expensive, such as Arbor Networks, Network Instruments.

Network traffic is received or sent, as mentioned above, the

information extracted from incoming and outgoing packets can be used to evaluate packet traffic [3] and in particular for effective prevention against a possible DDoS attack risk [6]. Therefore, how can we extract only the information that distinguishes between this type of attack, or which of the extracted information best describes this attack, or which information can be used to build an effective system to counter the DDoS attack? To answer these questions, we propose DDoS-Detector, a new algorithm that exploits only relevant data extracted from the traffic to detect DDoS attacks in real-time.

Our contribution focuses on improving the analysis and monitoring of network traffic, and is aimed at accelerating the detection of DDoS attack threats, and is designed to help analysts investigate past incidents offline. In addition, the document analyzes a set of data to provide the best set of features (these are high-quality features extracted from the data streams) to detect the attack in question.

The rest of this article is organized as follows. Section 2 presents work related to the detection of DDoS attacks. Section 3 contains a brief description of the DDoS attack and the technical basis for variable selection based on automatic learning. In section 4, the proposed approach is presented. Our experiences and results are contained in section 5. The conclusion of this paper is presented in Section 6.

II. RELATED WORK

In this section, we review the work that has been done to get an overview of approaches that may be applicable for analyzing network traffic to detect the DDoS attack.

Opeyemi Osanaiye et al [12] proposed a multi-filter feature selection method based on a set that combines the output of four filtering methods using a dataset intrusion detection marker, NSL-KDD and decision tree classifier, the results obtained show that their proposed method can effectively reduce the number of features from 41 to 13. Gavrilis Dimitris et al [6] uses a genetic algorithm to select 14 effective features from a set of 44 statistical characteristics and then use them to build a neural network-based DDoS detector. Eray Balkanli et al [1] used two algorithms, namely Chi-square and symmetric uncertainty for the selection of four different feature sets for each algorithm, as well as the decision tree classifier on four different training sets. Chundong Wang et al [18] proposed a DDoS detection system based on the SU-Genetic approach that classifies features according to the symmetric uncertainty and then selects the features with the genetic algorithm. They were able to reduce the number of features from 41 to 17 in the NSL-KDD dataset. A DDoS data detection approach has been proposed by Yonghao Gu et al [9] using a semi-supervised K-means algorithm which is based on a selection of hybrid features by (SKM-HFS) on four different data sets, namely, DARPA DDoS, CAIDA "DDoS attack 2007", CICIDS "DDoS attack 2017", and a real-world data set. Manjula Suresh et al [17] proposed a mechanism for selecting the most important features based on chi-square and information gain. Then, based on this selection they developed several types of machine learning models, such as Naives Bayes, C4.5, SVM, KNN, K-means and Fuzzy c-means clustering for the detection of DDoS attacks. Mihui Kim et al [8] proposed a combined data mining approach to model the traffic model of normal and diverse attacks to select important attributes to build a neural network-based model.

III. BACKGROUND

In this section, in the first part, we will define the DDoS attack, the different types of attacks as well as some technique to mitigate it, in the second part, we will briefly present a state of the art of techniques used for the selection of characteristics while citing the different algorithms best known in the literature.

A. Distributed Denial of Service

DDoS attacks [13] is short for Distributed Denial of Service is an attempt to make an online service unavailable by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. Their operation is most often based on botnets - a large group of distributed computers and other networked resources that act together - spamming simultaneously. The latter is effective in using multiple compromised computer systems as sources of attack traffic.

1) Types of DDoS Attacks: There are many types of DDoS attacks [7]. Attacks can however be divided into three categories:

Traffic attacks: Traffic flood attacks send a huge volume of TCP, UDP and ICPM packets to the target. As a result, the target undergoes an amplification of the pirate's initial request. As a result, legitimate requests are lost and these attacks can be accompanied by malware exploitation.

Bandwidth attacks: This DDos attack [3] overloads the target with massive amounts of unwanted data. This is because large amounts of data are sent to the target using some form of amplification or another means of creating massive traffic, such as requests from a botnet.

Application attacks: The objective of these attacks is to exhaust the target's resources. The attacks target layer 7 (about the 7th layer of the OSI model), leaving the target's system services unavailable.

2) Protection against DDoS attacks: As seen in the section above, DDoS attacks [7] have several types of attacks. One of the solutions available to virtually all network administrators is to create a route to a black hole and direct malicious traffic to that route. We can also limit the number of requests that a server will accept over a certain period. As a third solution, we cite the Web Application Firewall (WAF), which can act as a reverse proxy, protecting the targeted server against certain types of malicious traffic. By filtering requests based on a series of rules used to identify DDoS tools. Therefore, these rules can be defined according to a deep analysis of network traffic flow. On the other hand, the main difficulty

in mitigating a DDoS attack is to detect it, and this is due to the differentiation of attack (malicious) traffic from normal (legitime) traffic. This data flow is defended by a large number of Features that characterize internet traffic.

B. Feature selection approaches

The methods for feature selection are generally classified into three main categories: filter methods [20], wrapper methods [4], Embedded methods [19].

1) Filter methods: The principle of these methods is to evaluate each attribute according to a precise relevance score, then select the best attributes, that is to say the most relevant, As the algorithm FOCUS, Relief, LVF et Branch and bound [11].

2) Wrapper methods: Proposed by Kohavi and John in 1997 [13]. In these methods, the selection of features interacts with a classifier to find an optimal attribute subset for this learning model [10]. So the selected subset will be adapted to the classification algorithm used, Like SFS, SBS, Hill Climbing and Best first search.

3) Embedded methods: Embedded methods are close to Wrapping methods because they incorporate the selection of variables during the learning process. The difference is that in this method the classifier is used not only to assess a candidate subset but also to guide the selection mechanism. The Embedded methods can use all the learning examples [10] to establish the system. This is an advantage that can improve results. Decision trees [14] are the most suitable illustration of these methods.

The filtering methods tend to select similar characteristics, therefore, it does not avoid redundancy, as for the wrapping methods, they present limitations, on the one hand at the level of the complexity and the computation time necessary for the selection and on the other hand part by the dependence of the relevant characteristics selected on the classifier used.

IV. The architecture of the hybrid DDoS detection system

A hybrid method [3] is a research method made up of at least two separate research methods. The taxonomy of hybrid metaheuristics is divided into two parts: a hierarchical classification and a flat classification. The classification applies to deterministic methods as well as metaheuristics. These methods combine different concepts or components of various meta-heuristics. Indeed, metaheuristics are generally iterative stochastic algorithms, which progress towards a global optimum, i.e. the global extremum of a function, by sampling an objective function. Metaheuristics are generally iterative stochastic algorithms, ranging from simple local search to complex global search algorithms, i.e. the global extremum of a function, by sampling an objective function. among which we find the genetic algorithm.

In this section, we describe our system of DDoS detection. It is illustrated in Figure 1. It is based on two parts, a first part called ”offline” which performs a deep analysis of network traffic via a hybrid genetic algorithm called GA-TS (Genetic Algorithm Based on Taboo Search Strategy) to identify the most relevant feature clues that best characterizes the malicious traffic of the DDoS attack. Then, these will be used for two purposes at once, reducing the size of the dataset by removing additional information including (noisy, redundant, anomalies, outliers...) and selecting the features related to the clues in order to be able to build a traffic model in a supervised way based on the decision trees. This model will be trained and tested by dividing the reduced base into two bases, so the second purpose of the indices is to be used for the second part of the system, This will be done by indicating to the ”NetFlow extractor” to extract only the relevant information from the incoming traffic that will be used to build the new instances that will be examined by the DDoS-Detector that will classify them in an extra fast way either as legitimate (normal) traffic or malicious traffic that represents a DDoS attack and therefore trigger an alert to deal with this network traffic.

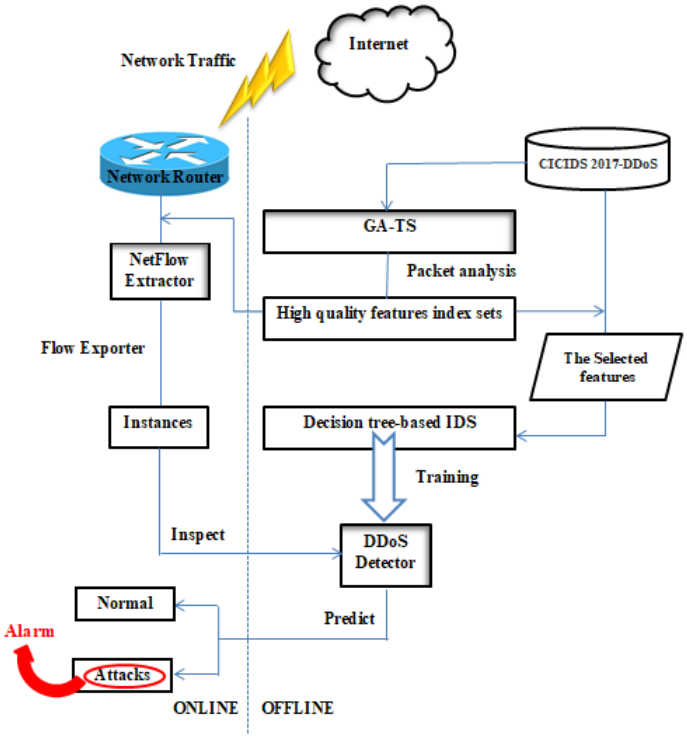

Fig. 1. DDoS detection system architecture.

V. Experimental results and discussion

A. Dataset Description

The CICIDS 2017-DDoS dataset [16] is used in this experiment, it consists of labeled network traffic, including complete packages in pcap format.

This is a dataset representative of real Internet traffic, the author [16] has defined dataset tasks sufficiently rich in both diversity and quantity. To generate this traffic, a regular session

and a session on DDoS attacks were launched. Therefore, we have 2 types of traffic, namely: 'BEGNIN' and 'DDoS', the first represents normal traffic while the second represents malicious traffic. The traffic was captured using Wireshark and tcpdump. In our experiments, we divided the dataset into two sub-bases in which the first one is 75% and for learning purposes while the second one is 25% for evaluation purposes. In the tables above, a brief description of the dataset used will be presented in Table 1 while Table 2 presents the information extracted from the network traffic.

Dataset	Training Set	Testing Set	Total
Instances	169308	56437	225745
Features	85	85	85
Normal Traffic	73352	24366	97718
DDoS Traffic	95956	32071	128027
Size (Mb)	55.12	18.38	73,5

TABLE I
DATASET DESCRIPTION.

B. The detection performance

There are several types of errors coming from a classifier influencing more or less its power. they can be summarized in the form of the following matrix of confusion (Table 3).

More precisely, we have to look at the costs of these errors.

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

$$Recall = \frac{TP}{TP + FN} \tag{2}$$

$$F_1 - score = \frac{2 * (Precision * Recall)}{Precesion + Recall} \tag{3}$$

$$DetectionRate = \frac{TP + TN}{TP + FP + TN + FN} \tag{4}$$

C. Results Analysis

This section focuses on the experiences and results that were carried out during this study. Note that all the experiments were programmed using the python 3 language on a machine that has 8 GB RAM, a processor Intel i7-4500U CPU @ 1.80GHz 2.4GHz on a 64-bit Windows operating system.

The initial population is randomly generated, the chromosomes of this population are represented as a binary vector of size n = 85, where n represents the number of initial characteristics, as shown in Figure 2. The chromosomal genes represent the features extracted from the network traffic and is equal to 1 if the feature corresponding to it is chosen and 0 otherwise.

At the beginning of the algorithm, we randomly generate a population of 20 individuals (the size of the population must not be large or it affects the speed of solving the problem). However, in each generation of the genetic algorithm, we

Id	Scale	Feature
f1	object	Flow ID
f2	object	Source IP
f3	integer	Source Port
f4	object	Destination IP
f5	integer	Destination Port
f6	integer	Protocol
f7	object	Timestamp
f8	integer	Flow Duration
f9	integer	Total Fwd Packets
f10	integer	Total Backward Packets
f11	integer	Total Length of Fwd Packets
f12	float	Total Length of Bwd Packets
f13	integer	Fwd Packet Length Max
f14	integer	Fwd Packet Length Min
f15	float	Fwd Packet Length Mean
f16	float	Fwd Packet Length Std
f17	integer	Bwd Packet Length Max
f18	integer	Bwd Packet Length Min
f19	float	Bwd Packet Length Mean
f20	float	Bwd Packet Length Std
f21	object	Flow Bytes/s
f22	object	Flow Packets/s
f23	float	Flow IAT Mean
f24	float	Flow IAT Std
f25	float	Flow IAT Max
f26	float	Flow IAT Min
f27	float	Fwd IAT Total
f28	float	Fwd IAT Mean
f29	float	Fwd IAT Std
f30	float	Fwd IAT Max
f31	float	Fwd IAT Min
f32	float	Bwd IAT Total
f33	float	Bwd IAT Mean
f34	float	Bwd IAT Std
f35	float	Bwd IAT Max
f36	float	Bwd IAT Min
f37	integer	Fwd PSH Flags
f38	integer	Bwd PSH Flags
f39	integer	Fwd URG Flags
f40	integer	Bwd URG Flags
f41	integer	Fwd Header Length
f42	integer	Bwd Header Length
f43	float	Fwd Packets/s
f44	float	Bwd Packets/s
f45	integer	Min Packet Length
f46	integer	Max Packet Length
f47	float	Packet Length Mean
f48	float	Packet Length Std
f49	float	Packet Length Variance
f50	integer	FIN Flag Count
f51	integer	SYN Flag Count
f52	integer	RST Flag Count
f53	integer	PSH Flag Count
f54	integer	ACK Flag Count
f55	integer	URG Flag Count
f56	integer	CWE Flag Count
f57	integer	ECE Flag Count
f58	integer	Down/Up Ratio
f59	float	Average Packet Size
f60	float	Avg Fwd Segment Size
f61	float	Avg Bwd Segment Size
f62	integer	Fwd Header Length.1
f63	integer	Fwd Avg Bytes/Bulk
f64	integer	Fwd Avg Packets/Bulk
f65	integer	Fwd Avg Bulk Rate
f66	integer	Bwd Avg Bytes/Bulk
f67	integer	Bwd Avg Packets/Bulk
f68	integer	Bwd Avg Bulk Rate
f69	integer	Subflow Fwd Packets
f70	integer	Subflow Fwd Bytes
f71	integer	Subflow Bwd Packets
f72	integer	Subflow Bwd Bytes
f73	integer	Init Win bytes forward
f74	integer	Init Win bytes backward

f75	integer	act data pkt fwd
f76	integer	min seg size forward
f77	float	Active Mean
f78	float	Active Std
f79	float	Active Max
f81	float	Active Min
f82	float	Idle Mean
f83	float	Idle Std
f84	float	Idle Max
f85	float	Idle Min

TABLE II
THE FEATURES SET OF THE CICIDS2017-DDOS DATASET.

	BENIGN	**DDoS**
BENIGN	TP	FN
DDoS	FP	TN

TABLE III
POSSIBLE CASES IN THE CLASSIFICATION.

evaluate each chromosome using our fitness function. We randomly select five parents from the initial population, we choose two parents among the 5, having the best cost provided by the evaluation function to perform the crossing. From these two individuals (parents) we obtain two new individuals (children).

In our case, the crossing is done from a single point with a very high probability of 0.9 indicating the reproductive participation rate. If the probability of crossing is 1, then the whole population participates in the crossing. And if it is 0, the new generation will be identical to the old population. Then to improve the generation of children, with a probability of 0.5 we move to the local search with the Descent algorithm of the first improvement, here we will call the taboo list to store the indices of genes that do not improve production to avoid cycling and this list will be emptied as soon as to genetically improve production, this is due to give the chance for a possible interaction between the different features. Finally, we move on to the mutation, it is done on a single gene chosen at random with a low probability of 0.1 allowing a diversification in the research space. In general, the genetic algorithm ends when the stop criterion is reached. In our case, the termination criterion is the number of generations set at 20.

1) Choice of fitness function: The definition of the fitness function is very important because the quality of each chromosome is evaluated by the latter, we have chosen the classification rate (Detection Rate, equation 4), because it gives a global overview of the state of the network traffic. The goal of our hybrid genetic algorithm GA-TS is to maximize this function, to do this we will use decision tree C4.5 [14] as a supervised learning algorithm to calculate the fitness value for each generation.

In this section, we analyze the results in terms of accuracy, precision, recall and F_1 score obtained in the testing and validation experiments (we used the validation data set to calculate each of the overall performances). The results of the test experiments are presented in Table 4 while the results of the validation experiments are presented in Tables 5 and 6. We compared our approach with 8 algorithms as reference methods.

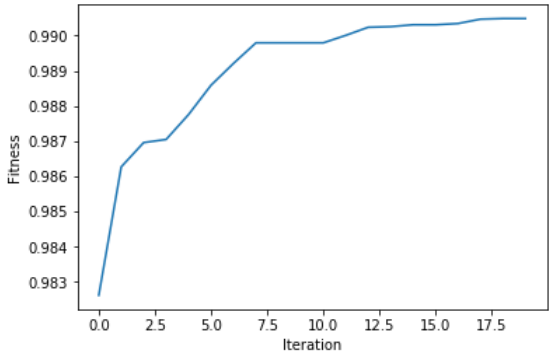

Fig. 2. Fitness Evolution according to the number of Features selected by the Hybrid Genetic Algorithm.

The curve (Figure 2) shows the evolution of the fitness value over the generations and indicates the convergence of the algorithm towards the best solution. This curve shows that the classification rate increases with the evolution of the population in each generation. The maximum value is reached in the 18th generation, we notice that the number of selected genes decreases, but overall the Fitness curve remains increasing.

Result of GA-TS:

From the results of this curve, we can notice that the result found shows that we were able to reduce the number of attributes by more than 78%. We get 19 features out of 85 that maximize the classification rate of the C4.5 algorithm, and the best solution is in the 18th generation. The following Table characterizes the results found:

Features set	f8	f12	f19	f23	f24	f28	f42	f43	f45
	f53	f54	f60	f61	f69	f72	f73	f75	f76
	f78								

TABLE IV
REPRESENTS RESULT OF FEATURES SET USING GA-TS.

	Precision	**Recall**	**F1-score**
BENIGN	1	1	1
DDoS	1	1	1

TABLE V
THE DETECTION PERFORMANCE OF THE DDOS ATTACK.

According to Table 5, we see that the DDoS attack was well-ranked with very high precision over 99% (1 is round rate). The proposed approach that was based on the hybrid genetic algorithm has a high success rate in choosing the best subset that features this attack as well possible, the model built based on reduced can know the normal traffic of illegitimate traffic (DDoS) at a detection rate of 99.6%.

Traffic type	BENIGN	DDoS
BENIGN	24359	7
DDoS	14	32057

TABLE VI
THE CONFUSION MATRIX USING THE DDOS-DETECTOR.

As illustrated in Table 6, we can see that 24359 was classified well as BEGNIN (normal traffic) but 7 was badly classified In return, 32057 was classified well for DDoS (illegitimate traffic) on the other hand 14 was considered like normal traffic.

In addition, we will make a quick comparison between the methods used in the following Table in the literature, in the same sense to reduce the complexity of the learning algorithms. We test the speed of these methods as well as the detection rate based on the random forest as estimators as well as the logistic regression algorithm as a detection model.

Search Method	Features	Run Time (Sec)	DetectionRate (%)
RFE	37	780	88.63
SBS	30	21600	90
Boruta	59	59797	92.65
SFM	22	33	93.95
GA-TS	**19**	12960	**95.9**

TABLE VII
COMPARISON OF BOTH SPEED AND DETECTION RATE OF FINDING FEATURE SUBSETS BY RFE, SBS, BORUTA, SFM AND GA-LS.

On the other hand, we will provide in the following Table comparison between the various Algorithms for literature detection. To do this, we based on the learning and testing time as well as the detection rate.

Algorithm	Training Time (Sec)	Testing Time (Sec)	DetectionRate (%)
LR	8.28	0.05	92.49
SGDClassifier	10.96	0.05	85.91
LDA	5.20	0.06	97.34
QDA	2.53	0.34	99.49
LinearSVC	81.87	0.05	96.52
SVM	504.41	21.32	99.87
GaussianNB	1.37	0.29	77
KNN	150	259.49	99.94
GA-TS-C4.5	1.96	**0,01**	**99.96**

TABLE VIII
THE PERFORMANCE EXAMINATION RESULTS.

VI. CONCLUSION AND PERSPECTIVES

In this article we have discussed the problem of DDoS attack detection, one of the main issues we have considered is how to choose an optimal subset of features that improves the analysis of network traffic in order to mitigate DDoS attacks. On the other hand, network traffic of data streams is characterized by 85 features. Indeed, the approach proposed in this paper could reduce the number of these features to more than 78% of the total number of features, this procedure of automatically selecting the features of the network traffic can reduce the cost of computation and training time, which ultimately leads to the improvement of the detection rate of DDoS attack detection. In the future, the performance of the hybrid genetic algorithm will be used for an in-depth analysis of the detection and classification of different types of DDoS attacks in network traffic.

REFERENCES

[1] Balkanli, E., Zincir-Heywood, A. N., & Heywood, M. I. (2015, October). Feature selection for robust backscatter DDoS detection. In 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops) (pp. 611-618). IEEE.

[2] Brownlee, N., Mills, C., & Ruth, G. (1999). Traffic flow measurement: Architecture. RFC 2722.

[3] Cherki, I., Chaker, A., Djidar, Z., Khalfallah, N., Benzergua, F. (2019). A Sequential Hybridization of Genetic Algorithm and Particle Swarm Optimization for the Optimal Reactive Power Flow. Sustainability, 11(14), 3862.

[4] Das, S. (2001, June). Filters, wrappers and a boosting-based hybrid for feature selection. In Icml (Vol. 1, pp. 74-81).

[5] Dash, M., Liu, H. (1997). Feature selection for classification. Intelligent data analysis, 1(1-4), 131-156.

[6] Dimitris, G., Ioannis, T., & Evangelos, D. (2004, May). Feature selection for robust detection of distributed denial-of-service attacks using genetic algorithms. In Hellenic Conference on Artificial Intelligence (pp. 276-281). Springer, Berlin, Heidelberg.

[7] Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm. IEEE Access, 7, 64351-64365.

[8] Kim, M., Na, H., Chae, K., Bang, H., & Na, J. (2004, February). A combined data mining approach for DDoS attack detection. In International Conference on Information Networking (pp. 943-950). Springer, Berlin, Heidelberg.

[9] Mirkovic, J., Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53..

[10] Michie, D., Spiegelhalter, D. J., Taylor, C. C. (1994). Machine learning. Neural and Statistical Classification, 13.

[11] Narendra, P. M., Fukunaga, K. (1977). A branch and bound algorithm for feature subset selection. IEEE Transactions on computers, (9), 917-922.

[12] Osanaiye, O., Cai, H., Choo, K. K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. EURASIP Journal on Wireless Communications and Networking, 2016(1), 130.

[13] Kohavi, R., John, G. H. (1997). Wrappers for feature subset selection. Artificial intelligence, 97(1-2), 273-324.

[14] Korting, T. S. (2006). C4. 5 algorithm and multivariate decision trees. Image Processing Division, National Institute for Space Research–INPE Sao Jose dos Campos–SP, Brazil.

[15] Saber, A., Fergani, B., & Abbas, M. (2018, October). Encrypted traffic classification: Combining over-and under-sampling through a PCA-SVM. In 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS) (pp. 1-5). IEEE.

[16] Sharafaldin, I., Lashkari, A. H., Ghorbani, A. A. (2018, January). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In ICISSP (pp. 108-116).

[17] Suresh, M., & Anitha, R. (2011, July). Evaluating machine learning algorithms for detecting DDoS attacks. In International Conference on Network Security and Applications (pp. 441-452). Springer, Berlin, Heidelberg.

[18] Wang, C., Yao, H., & Liu, Z. (2019). An efficient DDoS detection based on SU-Genetic feature selection. Cluster Computing, 22(1), 2505-2515.

[19] Wang, S., Tang, J., Liu, H. (2015, February). Embedded unsupervised feature selection. In Twenty-ninth AAAI conference on artificial intelligence.

[20] Zhang, D., Chen, S., Zhou, Z. H. (2008). Constraint Score: A new filter method for feature selection with pairwise constraints. Pattern Recognition, 41(5), 1440-1451.