Anomaly-Based DDoS Attack Detection by Using Sparse Coding and Frequency Domain

Ramin Fadaei Fouladi
Electrical and Electronics Engineering
Boğaziçi University, İstanbul, Turkey
Email: ramin.fadaei@boun.edu.tr

Orhan Ermiş
EURECOM
Sophia Antipolis, France
Email:ermis@eurecom.fr

Emin Anarim
Electrical and Electronics Engineering
Boğaziçi University, İstanbul, Turkey
Email: anarim@boun.edu.tr

***Abstract*—Distributed Denial of Service (DDoS) attacks have become one of the most significant problems that affects the user satisfaction by degrading the availability of on-line services. Although intrusion detection systems provide effective mechanism for discriminating various DDoS attacks, they become impotent of detection when bogus packets similar to normal ones are dispatched by the attacker. One idea is to model the normal behavior of the network traffic using time series representation of that traffic together with advanced statistical analysis techniques such as frequency domain analysis for detecting the occurrence frequency (energy) of each basic element in time series. However, frequency domain analysis may become inadequate if the original frequency features are used for the detection anomalies. Therefore, in this work, we propose a hybrid approach that employs frequency domain analysis with sparse representation model to find discriminative characteristics for anomaly-based DDoS detection. The proposed algorithm distinguish abnormal traffic from the normal one based on the energy of time series for the number of packets feature, which is extracted from the time series data by using the sparse representation model. Experimental results show that performance of the proposed algorithm provides better DDoS detection results than the state-of-the-art time-series based approaches in the literature.**

I. Introduction

With the increased popularity of cloud services, ensuring the availability of online services have become a significant issue due to the existence of Distributed Denial of Service (DDoS) attacks [1], [2]. In DDoS attacks, an attacker forms an army of distributed and connected devices called bots to overwhelm the traffic of a targeted network by masquerading source IP addresses of these devices to attack the targeted network in an untraceable manner. Therefore, incoming packets to the targeted network can be categorized as legitimate traffic for the protection mechanisms [3].

In order to protect online services from DDoS attacks, intrusion detection systems are employed as a defense mechanism. These systems can be categorized as signature-based intrusion detection and anomaly-based intrusion detection [4]. In the first approach, the detection mechanism is trained by the set of predetermined malicious traffic. Then, features of malicious traffic such as IP addresses of attackers, etc. are stored in a database to be used in the detection for subsequent attacks. When a new activity is detected, the database is queried whether or not determine the activity is malicious. On the other hand, in anomaly-based detection, the detection mechanism of an IDS is trained using the pattern of a normal activity. Then, any activity, which is out of the normal one is reported as the intrusion. Although traditional intrusion detection systems provide packet level analysis to extract features of the network traffic [5], they become impotent of detection with the new generation DDoS attacks that mimics legitimate network traffic.

Anomaly-based intrusion detection mechanisms are studied over the years [6]–[9]. One of the recent examples in this research is the study in [7]. The proposed approach uses the statistical measures of times series for the attack and the normal traffics to detect the DDoS attack. Another study in [8] uses entropy of time series to discriminate DDoS attacks. In [9], Qin et al. proposed the use of cluster modeling that jointly works with entropy of the time series. Frequency domain analysis of time series provides promising results for anomaly-based DDoS detection [10], [11]. The study in [10] employs Discrete Fourier Transform (DFT) [12] and Discrete Wavelet Transform (DWT) to extract frequency domain features of attack traffic and normal traffic from the network traffic time series. In [11], the Multi-Scale Principal Component Analysis algorithm is introduced for frequency domain analysis by employing wavelet transform and principal component analysis. Because of the complex spectral correlation of frequency features and the similarity between frequency domain attributes of attack and normal traffics, using the original frequency features to detect anomaly in the traffic, results in low detection performance. To address this problem, feature extraction step should be utilized to find discriminative characteristics. Sparse representation model is an effective method to transfer higher dimension vectors to the sparse vectors with a few non-zero elements. These lower dimension vectors would be used as the new feature sets which are expected to increase the performance of the anomaly detection [13]. Therefore,

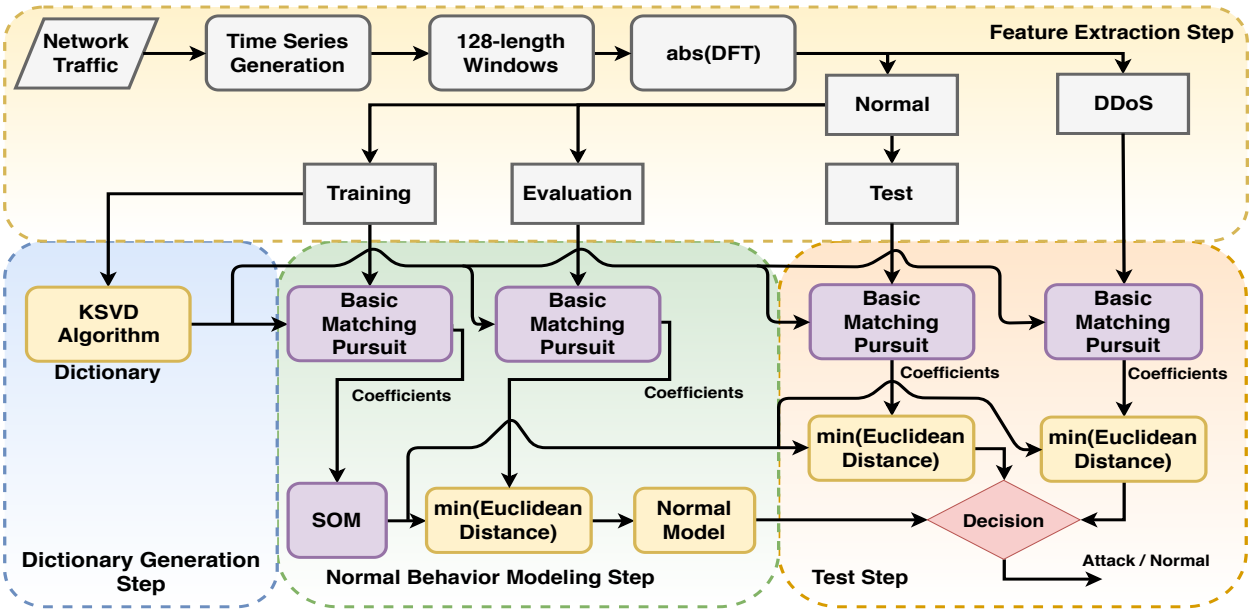


Fig. 1: An Overall View of the Proposed Model

we aim at combining frequency domain analysis with sparse representation model in order to increase the DDoS attack detection performance.

In this work, we propose an anomaly-based DDoS detection by using sparse representation model and frequency domain analysis. To the best of our knowledge, this is the first jointly use of these two methods for DDoS detection. The proposed model uses the absolute value of Discrete Fourier Transform (DFT) of the normal traffic to learn a sparse dictionary by employing K-SVD algorithm. Moreover, The sparse dictionary is employed by basic matching pursuit algorithm (BMP) to generate sparse coefficients of absolute value of DFT for both normal and attack traffics [14]. The normal behavior model is created by using sparse coefficients of the normal traffic and a self-organizing map (SOM) lattice [15]. Finally, we test the performance and the applicability of the proposed model by using CAIDA dataset [16]. Numerical evaluations show that the proposed model achieves high performance rates in terms of the detection performance.

The rest of the paper is organized as follows. The proposed model is introduced in Section II. Discussions and preliminary results are given in Section III. In Section IV, we discuss the detection performance of the proposed model. Finally, the paper is concluded in Section V.

II. The Proposed Model

In this study, we propose the improved version of DDoS detection approach in [10] by employing sparse coding to extract the most discriminating features from the frequency domain. Moreover, SOM Model is employed to create the normal behavior of the system. The overall view of the proposed model is as shown in Figure 1. The proposed method operates in Four steps, namely Feature Extraction Step, Dictionary Generation Step, Normal Behavior Modeling Step and Test step, which are defined as follows:

1) **Feature Extraction Step:** DDoS and Normal traffic samples from the input dataset are generated in this step. First, time windows are obtained by dividing the dataset into 128-millisecond windows. Then, for each window, absolute value (ABS) of DFT is estimated and is labeled as DDoS sample or normal sample. Later, Normal samples are divided as the training, the evaluation and the test parts in order to be used in the following modules.
2) **Dictionary Generation Step:** We employ K-SVD algorithm to generate the sparse dictionary of the normal samples. Dictionary is generated by applying K-SVD algorithm on the training part of normal samples that are already generated in the feature extraction module.
3) **Normal Behavior Modeling Step:** BMP algorithm is applied on both training and evaluation part of normal samples to estimate the sparse coefficients. Then, SOM model based on coefficients of the training part is generated and the empirical distribution of the minimum euclidean distance between neurons of SOM and coefficients of the evaluation part is used as the normal behavior of the system.
4) **Test Step:** BMP with the same dictionary of the previous part is executed on the test part of attack and normal traffics. In order to assign attack or

normal label for each test sample, the minimum euclidean distance between corresponding coefficients and the SOM lattice is calculated and compared with the normal behavior model.

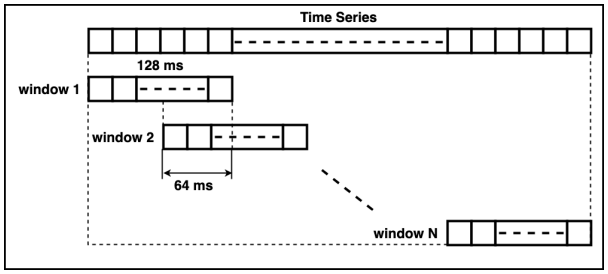


Fig. 2: Dividing time series into time windows

A. Feature Extraction Step

Feature extraction step of the proposed model operates as follows. First, the number of all arriving packets are counted for each $1ms$ time window in order to generate time series $\mathcal{P}_1^n$, where n is the total duration of the network traffic. Later, the time series, $\mathcal{P}$, is divided into $L = 128$ milliseconds length windows as $\mathcal{X}_{window\#} = \{x_1, x_2, \ldots, x_{128}\}$ with 64-length overlapped values with consecutive windows as shown in Fig. 2. Then, these windows are transferred into frequency domain by applying DFT which is accomplished by convolving the signal with complex exponential as given in the following equation:

$$X[f_n] = \frac{1}{L} \sum_{k=0}^{L-1} x_k e^{-j2\pi f_n T}, \tag{1}$$

where $x_k \in \mathcal{X}_{window\#}$ and $X[f_n]$ are the k^{th} element of the corresponding window and the energy of the window at f_n frequency bin, respectively. The output of DFT is a complex signal with the same length as input windows. Then, we use the absolute value of DFT as a feature. Since absolute value of DFT for a real signal is symmetric, we only consider one half of it, and therefore, for each window, we obtain 64 samples. Output samples of the feature extraction step are labeled as DDoS samples and normal traffic samples. The normal traffic samples are divided into three categories as training, evaluation and test samples to be used in the subsequent steps of the proposed model.

B. Dictionary Generation Step

The Dictionary Generation step operates on the training samples, which are obtained in the previous. We employ K-SVD algorithm [17] on training samples to generate an over-complete dictionary D. This dictionary is used to estimate the sparse coefficients of the samples. In sparse coding, an observation $y \in R^N$ can be modeled by $y \approx Dx$ where $D \in R^{N \times M}$ and $x \in R^M$ are dictionary matrices, and $k-$sparse vector respectively and $N < M$. By using $k-$ sparse vector, we guarantee that only $k \ll N$ elements in x become non-zero. The idea behind the sparse coding is to reconstruct y by using linear combination of k columns (or atoms) out of D. Then, x can be approximated by solving the following optimization problem:

$$\hat{x} = \underset{x}{\operatorname{argmin}} \|x\|_0 \quad s.t. \quad y = Dx \tag{2}$$

where $\|x\|_0$ is the l_0 pseudo-norm that counts the number of non-zero elements in x [17].

C. Normal Behavior Modeling Step

To generate the normal behavior model, first we obtain corresponding k number of coefficients by applying BMP algorithm on the training part of normal data using dictionary D. Then, Self-Organizing Map (SOM) algorithm [15] is applied on k coefficients to generate a SOM model. Finally, the evaluation part of normal traffic is processed in the BMP algorithm with the same D dictionary and the corresponding k coefficients are estimated. The set of the minimum euclidean distance between evaluation part coefficients and SOM model is used as the normal behavior of the system.

D. Test Step

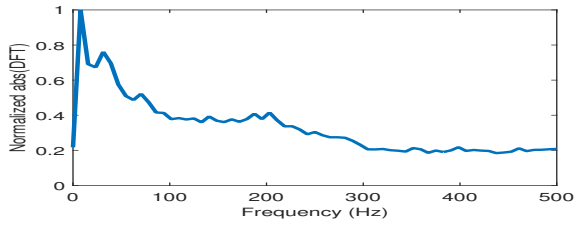
The performance of the proposed model is analyzed in this step. Since the dictionary D is generated by using the normal traffic data, we expect to have different sparse coefficients when applying BMP algorithm on the attack samples using this dictionary. Both test part of normal traffic and DDoS attack are fed to BMP algorithm with D as the sparse dictionary. The minimum euclidean distance between the coefficients of each sample and the SOM lattice is calculated and compared with the normal behavior model.

III. Discussions and Preliminary Results for CAIDA Dataset

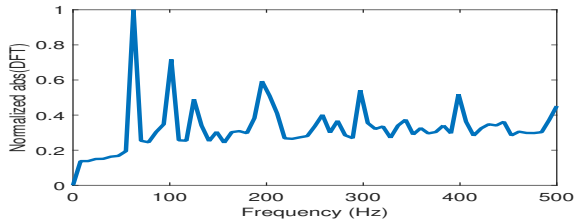
In this section, we give the discussions and preliminary results based on the application of the proposed model on CAIDA dataset with respect to sparse coding, normal behavior modeling based on sparse coefficients and SOM. The number of packets in each time intervals is the network feature which we employ in this work. The number of packets are counted per each $1ms$; therefore, according to the Nyquist theorem, the maximum frequency of received signal which can be realized for this sample rate, is $500Hz$. By 128-millisecond window, we achieve $7.8Hz$ frequency resolution, distributed in 64 bins.

Figure 3 displays an example of the normalized absolute value of DFT of number of packets for both normal and DDoS traffic of CAIDA dataset. Compared to the attack traffic in which has different dominant frequency bands, normal traffic tends to be a slow traffic. Both

the attack traffic and the normal traffic share different number of periodic components. DFT feature would not be a good choice for DDoS attack detection by itself and therefore, we use sparse coding for extracting discriminating features.



(a) Normal.



(b) Attack.

Fig. 3: Normalized Absolute Value of DFT (a) Normal, (b) DDoS Attack.

A. Sparse Coding by using K-SVD Algorithm for Dictionary Generation

As defined in Section II.B, an over-complete dictionary $D \in R^{64\times256}$, is estimated by applying K-SVD algorithm on the training part of the normal traffic data. D is initialized by using Gaussian random matrix and then it is processed by K-SVD algorithm. This dictionary is used by matching pursuit method to find the $k = 5$ coefficients of sparse coding for absolute value in DFT of the number of packets. k and the size of the dictionary D are selected empirically and by applying embedded feature selection method. Figure 4 displays the receiver operating characteristics (ROC) for different values of k. The discrimination accuracy of a model, can be related to the area under the ROC which is so called area under the curve (AUC). Considering this metric, the model with $k = 5$ outperforms compared to other values of k. By fixing k as 5, the performance of the model is analyzed by considering three different sizes of dictionary. Figure 5 displays the ROC results for different dictionary sizes. Dictionary with the size of 256 outperforms others with respect to AUC.

B. Normal Modeling Based on Sparse Coding Coefficients

In an anomaly detection approach, the model for the normal activity is obtained and used as the metric for spotting malicious activities. Any digression from normal behavior is considered as abnormality. One way to find the normal behavior of the network traffic is to utilize a learning algorithm. For this respect, we propose to use SOM algorithm as a learning algorithm in this work. Before modeling the normal behavior, the input data and the coefficients set obtained from basic matching pursuit are normalized with respect to the z-score of each observation. In order to create a SOM lattice, the size of the map should be specified. The number of neurons is determined by the number of observations in the training dataset using $Q \simeq 5 \times \sqrt{(O)}$ where Q and O are the number of neurons and the number of observations respectively [18]. From this observation, the number of neurons is selected to be 144.

Later, the SOM model is trained by the coefficients of normal training dataset. The number of iterations is assigned approximately as 500 times of the product of lattice dimension which is 72000 [15]. In the next step, the minimum euclidean distance between each coefficient of evaluation part of normal data and the neurons of the SOM are calculated and empirical probability distribution of those distances is utilized as the normal behavior of the system. Figure 6 represents the empirical probability density and normal Q-Q plot of the minimum euclidean distance of evaluation dataset from the neurons of the SOM model. From the Figure 6, we can infer that the model is heavy-tailed and right skewed.

Table I summarizes some statistical parameters of the empirical distribution. The Shapiro-Wilk (SW) test($P - value < 0.05$) and a visual inspection of the empirical pdf and normal Q-Q plot(Fig 6), show that minimum distances are not normally distributed. Moreover kurtosis ($5.54 > 3$) and skewness ($1.33 > 0$) indicate that distribution is fat-tailed (leptokurtic) and skewed to the right respectively. In the normal distribution extreme events are less likely than of fat-tailed one. This properties of fat-tailed distribution should be taken into account during the threshold value estimation. Underestimating this parameter would increase the false positive rate and

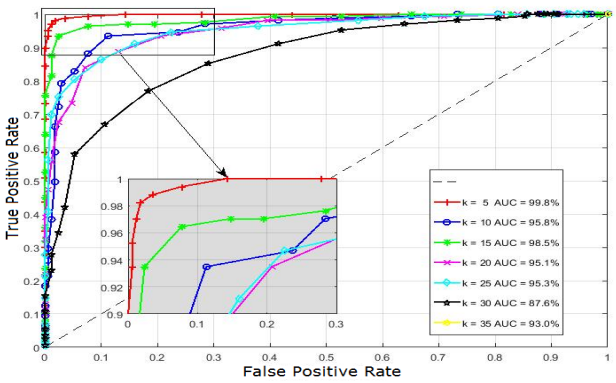


Fig. 4: ROC For Different Values of K={5,10,15,20,25,30,35}

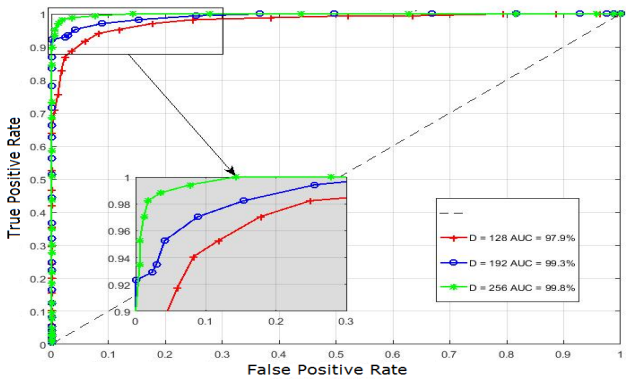
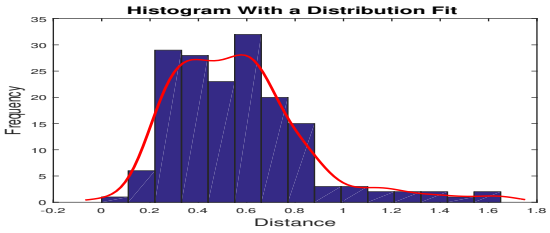
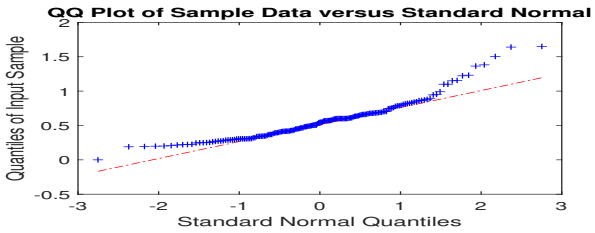


Fig. 5: ROC For Different Dictionary size of$\{128,192,256\}$ and $K = 5$



(a) Empirical pdf.



(b) Q-Q Plot.

Fig. 6: (a) Empirical pdf and (b) Q-Q Plot of Minimum Distance From Neurons of SOM Model.

decreases the DDoS detection performance.

IV. DDoS Detection Performance

In order to test the DDoS detection performance of the proposed model, we use CAIDA intrusion detection evaluation dataset [16]. Normal dataset is divided into three subsets as Training 796(70%), Evaluation 169(15%) and Test 169(15%). 169 TCP-based DDoS attack samples are used in the Test step. To analyze the performance of the proposed model, we use true positive (TP) and false positive (FP). While the former one corresponds to the total number of detected DDOS samples, the latter one corresponds to the total number of normal instances detected as attack samples.

TABLE I: Empirical pdf Statistics

No	Statistics	Value
1	Mean(M)	0.5646
2	Std	0.2697
3	M+2Std	1.1264
4	M+3Std	1.4073
5	Kurtosis	5.54
6	Skewness	1.33
7	Shapiro-Wilk P-Value	4.8E-4

The test dataset consists of normal and attack traffics, where each traffic has 169 samples. Five non-zero coefficients set of each test sample is estimated by using the dictionary D and BMP algorithm. In the next step, the minimum euclidean distance of each coefficient set from neurons of SOM model is found. Figure 7 displays the box plot of corresponding distances set. There are some points which reside outside the fence of the boxplot of the normal distances. These data points are located inside the boundary of attack distances which yields false alarms during the performance test. These distances are compared with the normal model which is the empirical distribution of distance of the normal evaluation part from the SOM model.

Table II summarizes the confusion table for different threshold values based on the standard deviation of the normal model. As the threshold value increases, the false positive (FP) value decreases but simultaneously, the detection deteriorates (True positive value(TP)). Selecting the 2 standard deviation of the mean value as the threshold to separate normal and attack data results in the best detection rate(TP); on the other hand, FP has the worst value. Although the 5 standard deviation of the mean value has the best FP, the detection rate of the model decrease significantly. Selecting the 3 standard deviation of the mean value as the threshold, gives the best result which is the trade off between TP and FP. The proposed algorithm achieves 1.2% and 99.4% of FP and TP respectively.

The performance of the proposed algorithm regarding to the overall accuracy, which is the total number of correct decision of the model, is compared with previous works. Table III, compares the accuracy of the proposed method with the previous works [7], [10]. In [7], Skewness has the best accuracy among considered statistical features. The model of naive Bayes with the input of the combination of DFT and DWT outperforms in [10]. Because the dataset used in [10] is different, we re-simulate the method. According to the Table III, the proposed method has the best prediction accuracy.

V. Conclusion

In this paper, we have proposed an anomaly-based DDoS detection by using sparse coding and frequency domain. A time series has been generated by counting the number of packets of CAIDA dataset for each $1ms$. The obtained time series has been further divided into 128-length widows which each new window shared first 64 samples with the previous one. The absolute

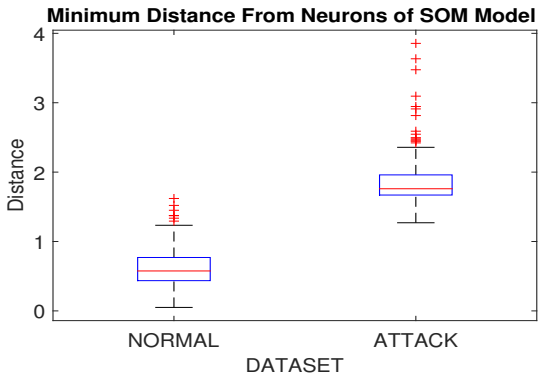


Fig. 7: Distance Box Plot

TABLE II: Confusion Table for Different Threshold Values.

Threshold		Normal	Attack
2Std(1.1264)	**Normal**	156	13
	Attack	0	169
3Std(1.4073)	**Normal**	167	2
	Attack	1	168
4Std(1.6434)	**Normal**	168	1
	Attack	54	115
5Std(1.9131)	**Normal**	169	0
	Attack	129	40

value of the DFT of windows have been employed as the dataset for this work. While normal data has been divided into three parts of training, evaluation and test, the attack data has been kept for the test step. An over-complete dictionary has been generated by applying K-SVD algorithm on the training part of the normal dataset. For each dataset including normal and attack traffic, five sparse coefficients have been estimated by using the obtained dictionary and BMP algorithm. The sparse coefficients of the training part of the normal data has been given as the input to the SOM algorithm to generate a SOM lattice. The minimum euclidean distance between sparse coefficients of each evaluation samples and the neurons of the SOM lattice has been calculated and its distribution has been used as the normal behavior. By comparing the minimum euclidean distance between the coefficients of each samples in the test part and SOM lattice, the performance of the proposed method has been analyzed. Our experimental results shows that the proposed algorithm provides 99.11% accuracy for DDoS attack detection and outperforms well-known studies in the literature. As a future work, we are planning to test the applicability of our approach in a real life scenario by applying our model to different DDoS attack datasets.

TABLE III: Comparison Between Accuracy Of Algorithms

Algorithm	Accuracy(%)
Proposed Algorithm	99.11
Algorithm in [7]	98.33
Algorithm in [10]	93.27

ACKNOWLEDGEMENT

This work is supported by the Turkish Ministry of Development under the TUBITAK project number 107R030..

REFERENCES

[1] S. Rai, K. Sharma, and D. Dhakal, "A survey on detection and mitigation of distributed denial-of-service attack in named data networking," in *Advances in Communication, Cloud, and Big Data*. Springer, 2019, pp. 163–171.

[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[3] G. Vormayr, T. Zseby, and J. Fabini, "Botnet communication patterns," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2768–2796, 2017.

[4] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," *arXiv preprint arXiv:1701.02145*, 2017.

[5] P. Shinde and S. Guntupalli, "Early DoS attack detection using smoothened time-series and wavelet analysis," in *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*. IEEE, 2007, pp. 215–220.

[6] "An intelligent intrusion detection system (ids) for anomaly and misuse detection in computer networks," *Expert Systems with Applications*, vol. 29, no. 4, pp. 713 – 722, 2005.

[7] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Statistical measures: Promising features for time series based DDoS attack detection," in *Multidisciplinary Digital Publishing Institute Proceedings*, vol. 2, no. 2, 2018, p. 96.

[8] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," *IEEE Communications Letters*, vol. 18, no. 1, pp. 114–117, 2014.

[9] X. Qin, T. Xu, and C. Wang, "DDoS attack detection using flow entropy and clustering technique," in *Computational Intelligence and Security (CIS), 2015 11th International Conference on*. IEEE, 2015, pp. 412–415.

[10] R. F. Fouladi, C. E. Kayatas, and E. Anarim, "Frequency based DDoS attack detection approach using naive bayes classification," in *Telecommunications and Signal Processing (TSP), 2016 39th International Conference on*. IEEE, 2016, pp. 104–107.

[11] Z. Chen, C. K. Yeo, B. S. L. Francis, and C. T. Lau, "A MSPCA based intrusion detection algorithm for detection of DDoS attack," in *Communications in China (ICCC), 2015 IEEE/CIC International Conference on*. IEEE, 2015, pp. 1–5.

[12] E. O. Brigham, *The Fast Fourier Transform and Its Applications*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1988.

[13] D. Ma, Y. Yuan, and Q. Wang, "Hyperspectral anomaly detection via discriminative feature learning with multiple-dictionary sparse representation," *Remote Sensing*, vol. 10, no. 5, p. 745, 2018.

[14] S. G. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionaries," *IEEE Transactions on signal processing*, vol. 41, no. 12, pp. 3397–3415, 1993.

[15] T. Kohonen, "The self-organizing map," *Proceedings of the IEEE*, vol. 78, no. 9, pp. 1464–1480, 1990.

[16] "Caida, 2011. the cooperative analysis for internet data analysis."

[17] M. Aharon, M. Elad, and A. Bruckstein, "K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation," *IEEE Transactions on signal processing*, vol. 54, no. 11, pp. 4311–4322, 2006.

[18] J. Tian, M. H. Azarian, and M. Pecht, "Anomaly detection using self-organizing maps-based k-nearest neighbor algorithm," in *Proceedings of the European Conference of the Prognostics and Health Management Society*. Citeseer, 2014.