IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 10, 2020, accepted June 17, 2020, date of publication June 29, 2020, date of current version July 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005781

Hybrid DDoS Detection Framework Using Matching Pursuit Algorithm

DERYA ERHAN, (Member, IEEE), AND EMİN ANARIM
Electrical and Electronics Engineering Department, Boğaziçi University, 34342 İstanbul, Turkey

Corresponding author: Derya Erhan (derya.erhan@boun.edu.tr)

This work was supported by the Scientific and Technological Research Council of Turkey (TUBİTAK) through the Cloud-Based Privileged Access Management Systems Project under Project 117R030.

ABSTRACT Although a considerable amount of research has been done on DDoS attacks, it still poses a severe threat to many businesses and internet service providers. DDoS attacks commonly generate a high amount of network traffic. However, the resource depletion DDoS attacks can deny the target service, although it generates much less traffic than legitimate traffic. We propose a novel DDoS detection framework using the Matching Pursuit algorithm to detect resource depletion type DDoS attacks. We use multiple characteristics of network traffic simultaneously in order to detect low-density DDoS attacks efficiently. The proposed method uses the dictionary produced from the parameters of the network traffic using the K-SVD algorithm.Dictionary generation using network traffic, provides legitimate and attack traffic models, and adds adaptability of the proposed method to network traffic. We also implement DDoS detection approaches that use Matching Pursuit and Wavelet techniques and compare them using two different data sets. Additionally, we offer a hybrid DDoS detection framework that combines these approaches with a decision-making mechanism using an artificial neural network. We evaluate the proposed methods with two different data sets. The proposed approaches perform over 99% true positive rate with a false positive rate lower than 0.7% with a low-density DDoS attack dataset. In the hybrid intrusion detection system with more than one attack, the detection performances of other methods have decreased, while the proposed approach achieves true positive rates higher than 99% with a false positive rate lower than 0.7%.

INDEX TERMS Artificial neural network, intrusion detection, DDoS, matching pursuit, K-SVD, wavelet.

I. INTRODUCTION

The exponential increase in the use of various applications over the internet led to a rise in security threats, such as Distributed Denial of Service (DDoS) attacks [1]. The DDoS attack aims to make an online service unavailable by consuming resources such as bandwidth, memory, or CPU of the target system.DDoS detection problem is a classic problem in the field of intrusion detection systems; therefore, there is a comprehensive prior art around the subject. However, DDoS attacks continue to be one of the biggest cyber threats affecting the financial, health, retail, gaming, and political sectors and resulting financial loss [2], [3]. In 2019 DDoS attack size increased 273%. In addition, 91% of the victims reported that the attack saturated their internet bandwidth. In April 2019, the most comprehensive network and application layer attack were seen with 580 million packets per second (PPS) [2]. Another attack lasted for 13 days and generated 292,000 Requests Per Second (RPS). Additionally, DDoS attack indicators increased by 84% in the last quarter of 2019 [3].

In general, DDoS attacks are divided into two groups of bandwidth depletion attacks and resource depletion attacks [4]. Bandwidth depletion attacks deny the service of the target system by flooding the target network with an excessive amount of packets. Resource depletion attacks aim to consume computing resources of the target system using malformed packets that exploit the network protocols. This work examines resource depletion flood type DDoS attacks.

Intrusion Detection Systems (IDS) are used to detect DDoS attacks. Intrusion detection methods are classified into two groups as anomaly detection and misuse detection according to their detection technique [5], [6]. Misuse detection

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Feng.

methods use patterns of attacks to identify the intrusions. Anomaly detection methods use attack-free network traffic patterns to identify the attack. Hybrid intrusion detection combines anomaly and misuse detection methods. We perform both anomaly and misuse type of detections on DDoS attacks. The methods are combined with the decision module for the detection of multiple DDoS attack classes to form a hybrid detection mechanism. The decision engine is also combined with the Wavelet and the Matching Pursuit Mean Projection (MPMP) methods to compare similar signal representation methods. Performances of these three approaches are compared with each other using the CAIDA [7], [8], and Boğaziçi University DDoS attack dataset (BOUN DDoS) [9].

MP is a greedy algorithm that represents any signal as a linear expansion of atoms chosen from a redundant dictionary [10]. MP finds linear approximations of signals, by iteratively projecting them over a set of atoms selected from the dictionary. It may give a suboptimal approximation. However, MP is useful when it is hard to come up with an optimal orthogonal solution.

In this study, we discuss Wavelet and MP based DDoS detection approaches. These are, MPMP, Adaptive Matching Pursuit Based Detection (AMP), and Wavelet-based intrusion detection methods. Initially, we evaluated and compared these approaches using the CAIDA datasets. CAIDA datasets are used as a combination of two datasets containing only DDoS attacks and only attack free traffic. CAIDA datasets are frequently used for the evaluation of DDoS detection methods, and they include high DDoS attack density. These methods were evaluated and compared using the BOUN DDoS dataset, which has a lower DDoS attack intensity. We combine these methods with a decision-making mechanism using Artificial Neural Network (ANN) to form a hybrid intrusion detection system. We evaluate the hybrid framework with datasets containing TCP SYN flood and UDP flood attacks. In addition, we combine these datasets and evaluate the performance of the hybrid framework using the combined dataset containing both TCP and UDP attacks.

We first introduce the AMP approach in [11]. The AMP method has many advantages compared to MPMP and Wavelet-based DDoS detection approaches. AMP introduces the characteristic feature vector to design a method that uses multiple traffic characteristics concurrently. Additionally, instead of using the predefined structural dictionaries, the AMP generates dictionaries from the training dataset. We perform anomaly and misuse detection approaches using the dictionaries generated from normal and attack traffic using the AMP approach. Unlike previously proposed work, AMP detects attacks using residuals obtained from the MP algorithm.

The contribution of this study can be listed as follows:

- We combine anomaly detection and misuse detection in the AMP method using a decision engine. We also combine one-dimensional traffic attributes with the decision engine in Wavelet and MPMP methods.
- We reimplement DDoS detection methods using Wavelet and MPMP and compare it with the AMP approach.
- We use two different datasets for evaluating and comparing the methods.
- We evaluate both methods with and without the decision engine for the detection of TCP and UDP flood attacks.
- We also combine TCP and UDP flood datasets to evaluate the performance of the methods in the detection of DDoS attacks in three traffic classes.

This paper is organized as follows. Section II gives a brief description of related work on DDoS detection approaches using the MP algorithm. Section III explains the concept of the MP algorithm briefly and gives information about datasets and evaluation parameters. Section IV explains the methodology of MPMP, Wavelet, AMP, and Hybrid Detection framework. Section V includes the evaluation and comparison of the DDoS detection methods using 2 different datasets. Section VI presents our conclusions.

II. RELATED WORK

Detection of DDoS attacks using the MP algorithm is first implemented using the MPMP of the reconstructed network signal [12]–[15]. Renk *et al.* proposes an attack detection framework that utilizes the MP algorithm to create profiles of attack and legitimate traffic in [16]. MPMP-based DDoS detection approach is compared with different signal representation methods (e.g., Discrete Wavelet Transform) in [19]. Also, DDoS detection using MP and Orthogonal Matching Pursuit (OMP) algorithms is proposed in [15]. The OMP algorithm, principal component analysis, robust principal component analysis, and backpropagation neural network methods are used for DDoS detection in [18].

Network anomaly characteristic models using a basis pursuit based methodology is used in [17]. They generate anomalous and non-anomalous basis functions to construct a dictionary from labeled data using Discrete Cosine Transformation and Wavelet basis. They use synthetic traffic data, GEANT network backbone router traffic, byte counts recorded from the Abilene Internet2 backbone network.

We first published the AMP method in [11]. Unlike other approaches, the AMP approach differs from other approaches because it uses multiple network traffic features, uses a network-generated dictionary, and generates alarms from residuals. Dictionary generation from traffic data provides the adaptation of AMP-based DDoS detection to network traffic. The focus of this study is the development of the AMP method and its comparison with other methods.

We summarise methods, datasets, and remarks from literature using MP for DDoS detection in Table 1. As we can see from the table, the MPMP and Wavelet methods are essentially used for DDoS detection. In order to compare the

TABLE 1. DDoS detection with sparse signal representation in the literature.

Reference	Methods	Dataset	Abnormality Value	Remarks
[12]	MP	MAWI, CAIDA	MPMP	Gabor Dictionary is used, DDoS Detection
[13]	MP , DWT	MAWI, CAIDA	MPMP, Energy of sub-bands	Gabor Dictionary is used, worm detection
[14]	MP , KSVD	DARPA , CAIDA, KDD	MPMP, Energy of Dictionary Elements	Dictionary is constructed with K-SVD
[15]	MP , DWT	MAWI, CAIDA	MPMP, Energy of sub-bands	Gabor Dictionary is used, DDoS Detection
[16]	MP	Simulated Dataset	MPMP	Gabor Dictionary is used, DDoS Detection
[17]	OMP	Synthetic Traffic Data, GEANT, Abliene Real-World Data	Corresponding dictionary atoms	Anomalous and non-anomalous dictionary atoms are generated.
[11]	MP , KSVD	BOUN DDoS	Residual of MP obtained from different dictionaries.	Residuals obtained fromMPis used as detection scores
[18]	PCA, OMP, ANN,	Synthetic Traffic Data, Janepese SIP real data.	Residual error	They create basis functions using SVD.

AMP approach and the Hybrid DDoS Detection Framework, we choose MPMP and Wavelet methods.

III. BACKGROUND INFORMATION

In this section, the concepts of MP and Wavelet-based detection of DDoS attacks and which are used in this work are discussed briefly. We also give brief information about Artificial Neural Networks and datasets used in this paper.

A. MATCHING PURSUIT ALGORITHM

MP is a sparse signal representation method that finds linear approximations of signals, by iteratively projecting them over a set of atoms selected from the dictionary. The dictionary of the MP algorithm can be a predefined structured dictionary built from a mathematical model. Also, the dictionary can be generated directly from sample data. Structured predefined dictionaries consist of atoms formed from expansions of a single basis, such as Wavelet or Fourier. On the other hand, generating the dictionary from sample data often leads to better representation and can yield better results in many practical applications [20].

To achieve a sparse representation of a given signal $\boldsymbol{y} \in \mathbb{R}^n$ using an over-complete dictionary $\boldsymbol{D} \in \mathbb{R}^{nxK}$, we define the representation of $\boldsymbol{y} = \boldsymbol{Dx}$ or $\boldsymbol{y} \approx \boldsymbol{Dx}$ subject to $\| \boldsymbol{y} - \boldsymbol{Dx} \|_p \leq \epsilon$ for some small number ϵ.

The sparsest representation is the solution to either [21]:

$$\min_x \| \boldsymbol{x} \|_0 \quad subject\ to\ \boldsymbol{y} = \boldsymbol{Dx}, \tag{1}$$

or

$$min_x \| \boldsymbol{x} \|_0 \quad subject\ to\ \| \boldsymbol{y} - \boldsymbol{Dx} \| \leq \epsilon, \tag{2}$$

where $\| . \|_0$ is the L_0 norm of a vector.

The MP algorithm decomposes any vector $\boldsymbol{y} \in \mathbb{H}$ in a Hilbert space over a redundant dictionary $\boldsymbol{D} = \boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2 \ldots, \boldsymbol{\alpha}_K \subseteq \mathbb{H}$, where $\boldsymbol{\alpha}_i \in \mathbb{H}$ is an atom in the dictionary, i is the index of the atom, and $\boldsymbol{x} \in \mathbb{R}^K$ contains the representation coefficients of $\boldsymbol{y}$.

In the first step, to achieve the best sparse decomposition of signal $\boldsymbol{y}$, we have to find atom $\boldsymbol{\alpha}$ that has the highest inner product with the signal $\boldsymbol{y}$. First residual $\boldsymbol{r}$ is equal to the entire signal $\boldsymbol{r}_0 = \boldsymbol{y}$. In order to minimize the energy of residual $\boldsymbol{r}_1$, the algorithm starts with finding α_0 that gives a maximum projection of $\boldsymbol{y}$

$$\boldsymbol{\alpha}_0 = \arg\max_{\boldsymbol{\alpha}_i} \langle \boldsymbol{y}, \boldsymbol{\alpha}_i \rangle \tag{3}$$

The residual is updated by subtracting $\boldsymbol{\alpha}_0$ times its magnitude of projection c_0 from $\boldsymbol{y}$:

$$\boldsymbol{y}_1 = \boldsymbol{y} - c_0 \boldsymbol{\alpha}_0 \tag{4}$$

where $c_0 = \langle \boldsymbol{y}, \boldsymbol{\alpha}_0 \rangle$ is called coefficient of $\boldsymbol{\alpha}_0$ This process continues iteratively by projecting $\boldsymbol{r}_i$ on dictionary atoms and updating $\boldsymbol{r}_{i+1}$. After m iterations $\boldsymbol{y}$ can be written as :

$$\boldsymbol{y} = \sum_{i=0}^{m-1} c_i \boldsymbol{\alpha}_i - \boldsymbol{r}_m \tag{5}$$

The residual can be written as:

$$\boldsymbol{r}_m = \boldsymbol{y} - \boldsymbol{Dx} \tag{6}$$

Conservation of energy is also retained providing:

$$\|\boldsymbol{y}\|^2 = \sum_{i=0}^{m-1} \|c_i\|^2 + \|\boldsymbol{r}_m\|^2 \tag{7}$$

The $\| \cdot \|^2$ in equation (7) is the L_2 norm of the vector. The approximations can be refined by orthogonal MP, tree-based orthogonal MP, or flexible tree search orthogonal MP. We prefer the basic MP algorithm in order to decrease experimental complexity.

B. EVALUATION PARAMETERS AND DATASETS

The methods are evaluated using CAIDA and BOUN DDoS datasets. CAIDA 2008 dataset contains anonymized bidirectional traffic traces. CAIDA 2007 dataset contains approximately one hour of anonymized traffic traces from resource depletion DDoS attack.

BOUN DDoS dataset is generated in the Boğaziçi University campus network via hping3 software. Aside from the data sets we use, there are various data sets utilized in the DDoS detection research area. These are KDD [22], MAWI [23], and DARPA [24] datasets. The BOUN DDoS dataset is newer than KDD and DARPA datasets. Unlike other datasets, the BOUN DDoS dataset includes multiple low-density DDoS attacks in different intensities that attack free traffic in the background. In the BOUN DDoS dataset, the attack is maintained through one victim server inside the campus of Boğaziçi University. The dataset was recorded in the backbone router of the campus, and it contains various types of legitimate traffic in addition to DDoS attacks. There are SYN Flood and UDP Flood attacks in the BOUN dataset. There is no publicly available DDoS dataset that contains more than one type of flood attack except the BOUN DDoS dataset. Because of this, we have to use the BOUN dataset for multiple traffic class cases. BOUN DDoS dataset is a new dataset available online and used in academic papers [25]–[29]. These datasets are divided into two subsets as training and test. The training dataset contains 30% of the whole dataset, while the test dataset contains 70%.

Five different metrics, including true positive rate (TPR), false-positive rate (FPR), Receiver Operating Characteristic (ROC) curve, Area Under ROC curve (AUC), and Accuracy (Acc) are calculated for evaluation detection of the methods.

These metrics are calculated using the number of correctly identified samples and the number of missed samples by the detector. True positive (TP) corresponds to attack samples classified as an attack, while true negative (TN) samples are attack-free samples classified as normal. Similarly, false-positive (FP) corresponds to attack-free samples falsely classified as an attack, while a false negative (FN) corresponds to attack data classified as normal. The evaluation parameters are calculated as follows:

$$TPR = \frac{TP}{TP + FP} \tag{8}$$

$$FPR = \frac{FP}{FP + TN} \tag{9}$$

$$Acc = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

These metrics are incapable of finding the best operating point of the detection system. For this reason, we employ Capability of Intrusion Detection (*CID*) metric [30] to find the best operating point. *CID* parameter takes into account all the fundamental aspects of evaluation metrics and subtle changes on these metrics, including TPR, FPR, positive predictive value, negative predictive value, and base rate. A higher *CID* value means that the IDS has a better capability of classifying input events accurately. We select the point in the ROC curve that gives the maximum *CID* value for comparison of detection performances. Operation points for the performance metrics in the results section are chosen according to the highest CID value.

Let X be the random variable representing the IDS input and Y the random variable representing the IDS output. The entropy of the input of the random variable X is defined as [31]:

$$H(X) = -\sum_{x \in X} p(x) log(p(x)) \tag{11}$$

The mutual information [31] between random variables X and Y is defined as:

$$I(X; Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) log \frac{p(x, y)}{p(x)p(y)} \tag{12}$$

Using equations (11), and (12) we can calculate *CID* as:

$$CID = \frac{I(X; Y)}{H(X)} \tag{13}$$

The mutual information measures the reduction of uncertainty of the input by knowing the IDS output. Besides, this mutual information is normalized with the entropy of the input, $H(X)$. Thus, CID is the ratio of the reduction of uncertainty of the IDS input, given the IDS output. Its value range is [0, 1].

IV. DDoS DETECTION USING AMP, MPMP, AND WAVELET APPROACHES

A. FEATURES AND FEATURE GENERATION

Packet flowing throughout the network contains various properties, including source-destination IP addresses, TCP flags, and source/destination ports, traffic flow information [40]. This diversity results in high dimensional attribute space. Attribute diversity examples include traffic flow information [41], [42], router SNMP MIB variables [43], TCP header information [44], entropy-based features [45]. One of the challenges about attributes is to find the best set of features that represents different types of DDoS attacks from a wide variety of a set of attributes. Besides, multiple traffic attributes are subject to change simultaneously under DDoS attack [46]–[48].

In the feature generation phase, we extract numerical traffic attributes from the dataset that contains raw network packets. Initially, we divide network traffic into equally spaced time windows. Then we count some specific properties of network packets in the time window and form attribute vectors $\boldsymbol{f}$ defined in Table 2.

TABLE 2. Traffic attributes and descriptions.

Attribute Name	Description
Number of SYN packets [32]	The number of packets that have SYN flag bit set to 1 per time window.
Number of RST packet	This attribute includes the number of packets that have RST flag bit set to 1 per time window.
Number of ACK packets	This attribute includes the number of packets that have ACK flag bit set to 1 per time window.
Number of packets [33], [34]	This attribute includes the number of packets that have ACK flag bit set to 1 per time window.
Average packet size [35]–[37]	This attribute corresponds to average packet size of packets in time window.
Data Transferred	This attribute includes total payload in bytes going through the network per time window.
Number of TCP, UDP, and ICMP packets	This attribute represents the number of TCP, UDP, and ICMP packets per time window and can be used to distinguish TCP, UDP, and ICMP attacks from each other.
Number of hosts [38]	This attribute represents the number of unique source and destination IP addresses per time window.
Number of flows [39]	This attribute represents the number of unique communicating pairs (flows) per time window.
Packet per-flow	This attribute contains the average number of packets per each unique flow per time window.
Data per-flow	This attribute contains the amount of data in bytes flowing in each unique flow per time window.
TCP, UDP, ICMP packet per flow	This attribute includes packet count per flow regarding their transfer layer protocol.

The network traffic is handled in two different ways in this work as traffic attributes and characteristic feature vector. One-dimensional attribute vectors are affected by DDoS attacks in various ways. The effect of DDoS attack on the attributes varies according to the intensity/type of the attack, size of the victim network, and the variety of attacking IP addresses. Sixteen different flow-based and packet-based traffic attributes are obtained from network traffic. The attributes used in this study are chosen based on their potential to reveal the properties of DDoS attacks. The explanations of these attributes and some of the academic studies using these attributes are shown in Table 2.

Packet-based attributes are obtained by computing the characteristics of the packets in the network traffic. Flow information is not taken into account while generating these attributes. The packet-based attributes are the number of SYN, RST, ACK, TCP, UDP, and ICMP packets. These are counted using packet header information.

Traffic flow is characterized as a sequence of packets that share common properties, such as the same source/destination IP addresses and source/destination ports. In this work, network flows are created by considering source/destination IP address pairs and source/destination TCP ports pairs of network packets. The flow-based attribute vectors used in this work are the number of flow, packet per flow, data per flow, and TCP, UDP, ICMP packets per flow. Here while calculating average packet size, data is counted as the length of the payload of the packets.

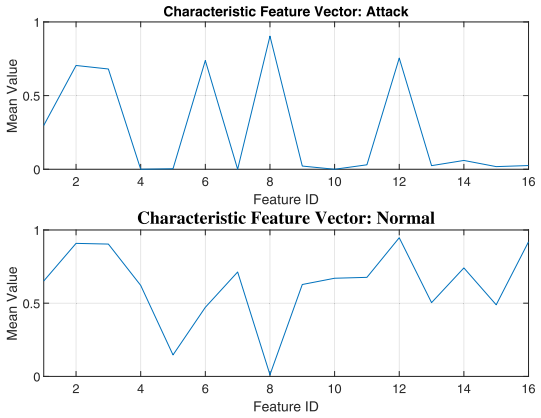

FIGURE 1. Mean of the characteristic feature vectors for Attack and Normal samples in CAIDA'07 and CAIDA'08 dataset.

To capture the effect of DDoS attacks on different traffic attributes simultaneously, we propose the characteristic feature in this work. The main idea behind building this feature is to model characteristic behaviors of the attributes of normal and attack traffic for every time window. The characteristic feature vectors obtained from the attack data differ from those obtained from attack-free data, as seen in Figure 1.

For every time window, a characteristic feature vector is generated. Every attribute vector is normalized within itself and combined to form characteristic feature vectors

as follows:

$$\mathbf{y}_i = \{\hat{f}_{1i}, \hat{f}_{2i}, \ldots, \hat{f}_{ni}, \ldots, \hat{f}_{16i}\}, \quad i = \{1, 2, \ldots, k\} \quad (14)$$

where, $\hat{f}_{ji}$ is the i^{th} element of j^{th} normalized attribute vector $\hat{\boldsymbol{f}}$. The attribute index j ranges between 1 and 16 because there are 16 attribute vectors.

B. DDoS DETECTION USING MPMP AND WAVELET

Previous studies in MP based DDoS detection field focus on MPMP. In this work, we reimplement DDoS detection methods using MPMP and Wavelet approaches covered in [15]. Furthermore, we compare the AMP-based DDoS detection with MPMP based and Wavelet-based DDoS detection methods.

The following details should be considered in the evaluation of these methods.

- MPMP and Wavelet methods use one-dimensional traffic attribute vectors. These two methods are applied to each attribute vector separately, and different results obtained for each attribute vector. Only the best performance achieved with these methods are included in the evaluation of these methods in this paper. In comparison, the AMP approach incorporates the information of multiple attributes using characteristic feature vectors.
- MPMP and Wavelet methods perform detection utilizing the energy changes of attribute vectors. The AMP approach uses dissimilarities in characteristic features of legitimate and attack traffic.

1) DDoS DETECTION USING MATCHING PURSUIT MEAN PROJECTION

Structured predefined dictionaries are commonly used in matching pursuit methods. The anomaly detection method proposed in [16] practices a dictionary that consists of atoms of Gabor base functions. Gabor base functions provide optimal joint time-frequency localization. A real Gabor function can be expressed as:

$$g_\gamma(t) = K(\gamma)\exp\{-\pi(\frac{t-u}{s}))\sin(2\pi\frac{w}{N}(t-u)+\phi) \quad (15)$$

where N is the size of signal for which dictionary, $K(\gamma)$ is normalizing constant to achieve atom unit energy such that $\|g_\gamma\| = 1$

$\gamma = \{u, w, s, \phi\}$ denotes parameters of the dictionary functions corresponding time, frequency, scale, and time shift. Dictionary used to calculate MPMP consist of one dimensional Gabor base functions. The dictionary, $\boldsymbol{D}$ is built using ten different scales and 50 different frequencies, to create an over-complete set of base functions. One dimensional traffic attributes are partitioned into signal windows of 10. This signal is decomposed with the use of the MP algorithm and structured Gabor dictionary. After MP decomposition, we achieve projection coefficients of c_k, which are used for creating normal traffic profiles. MP algorithm give 3 outputs corresponding atoms $\boldsymbol{\alpha}$, residues $\boldsymbol{r}$ and weights c. Matching pursuit mean projection is defined as:

$$MPMP = \frac{1}{M}\sum_{i=0}^{M-1} c_i \quad (16)$$

The main idea behind this approach is to utilize the relation between the energy of the signal and MPMP. If the energy of the specified attribute increases, the MPMP value also increases. The difference between MPMP of the time window in the test dataset and the average MPMP obtained from attack-free samples in the training dataset is used as an anomaly indicator value. When this value exceeds a certain threshold, an alarm is generated.

2) DDoS DETECTION USING WAVELET

Wavelet decomposition represents a signal using a series of orthogonal wavelets. For detection of DDoS attacks using Wavelet, we decompose the input signal into subbands and calculate the differences of energies of sub-bands. The concept of Wavelet transform was defined in [49] as follows:

$$W_d f(m, n) = \sum f(x).\Psi_{m,n}(x), \quad (17)$$

where $\Psi_{m,n}$, means a family of discrete Wavelet functions. Detection method in this section is proposed in [15]. Deaubechies type Wavelet is used to decompose network traffic features as proposed in [15]. Detection is performed by using energy of three DWT sub-bands $E_W(i)$ using approximation coefficients $\boldsymbol{ca}_1, \boldsymbol{ca}_2, \boldsymbol{ca}_3$. The energy of i^{th} sub-band, $E_W(i)$ using K coefficient is calculated as:

$$E_W(i) = \sum_{n=1}^{K} \boldsymbol{ca}_i^2(n) \quad (18)$$

The difference En between $E_W(i)$ of three different subbands are used as an abnormality indicator value for the Wavelet-based detection approach. Alarms are generated by thresholding abnormality indicator value En.

C. PROPOSED ADAPTIVE MATCHING PURSUIT BASED DDoS DETECTION

In this section, we give detailed information about the AMP approach. The AMP approach contains three main parts, namely Feature Generation Module, Dictionary Generation Module, and Alarm Generation Module. Figure 2 shows the block diagram of the AMP approach.

The feature generation module extracts attributes of network packets from network-based traffic data. The module partitions the dataset into equally spaced time windows and calculates 16 attributes for every time-window. The characteristic feature vectors are created from the normalized attribute vectors. Characteristic feature vectors obtained from the training dataset are classified into multiple classes depending on whether they belong to normal or attack traffic.

The dictionary generation module generates dictionaries from training data. Generating dictionaries from network traffic provides the adaptation of the AMP method to training data. Separate dictionaries are generated from different traffic classes.

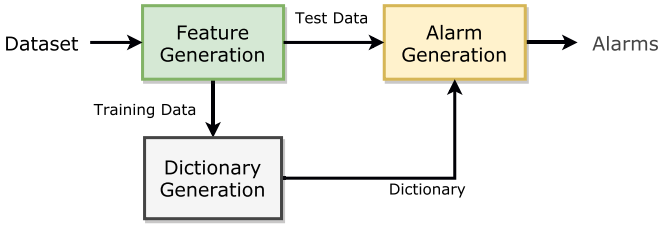

FIGURE 2. Block diagram of the AMP DDoS Detection approach.

The alarm generation module calculates the norms of residuals for every time window and generates abnormality values.

1) DICTIONARY GENERATION

Different types of dictionaries are generated from the training dataset in this work. From attack samples of feature vectors in training data, a misuse dictionary is generated. Similarly, from the attack-free samples of feature vectors in training data, an anomaly dictionary is created. Figure 3 shows the block diagram of the dictionary generation process.

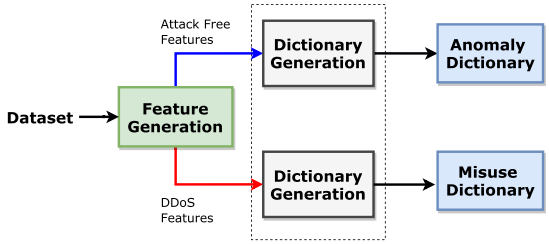

FIGURE 3. Block diagram of dictionary generation module.

To obtain dictionaries, an iterative optimization algorithm K-SVD is used. K-SVD is a generalized k-means clustering algorithm proposed in [21], [50]. In the dictionary generation process, a dictionary that consists of K atoms is produced from the training set of features. Dictionary size is determined experimentally in this work. Lets construct a matrix $\boldsymbol{Y}$ from characteristic feature vectors obtained from training dataset. The objective function of the K-SVD algorithm is as follows:

$$\min_{\boldsymbol{D},\boldsymbol{x}} \| \boldsymbol{Y} - \boldsymbol{D}\boldsymbol{x} \|_F^2 \quad subject\ to\ \forall i, \| \boldsymbol{x}_i \|_0 \leq \epsilon \tag{19}$$

where, $\| \ . \ \|_F^2$ is Frobenius norm, and $\| \ . \ \|_0$ is the L_0 norm of a vector. According to the equation (19), the K-SVD algorithm aims to produce the dictionary that gives the smallest residual value in Frobenius norm sense using the given data set. The training dataset can contain different traffic classes like attack-free traffic class and various types of attacks. For every traffic class, a separate dictionary is created. As a result, Frobenius norms of the residuals obtained using these dictionaries of a specific traffic class, have smaller values for vectors that are in the same category. Similarly, the vectors of different traffic classes result in higher norms.

2) ALARM GENERATION

For every time window in the test dataset, a characteristic feature vector is obtained using the feature generation module. These feature vectors are decomposed by the MP algorithm using the dictionaries obtained from the dictionary generation module. The abnormality indicator value is calculated from the resulting residual vectors as follows:

$$\psi_i = \| \boldsymbol{r}_i \|^2 \tag{20}$$

where ψ_i is the abnormality indicator value obtained for i^{th} time window, and $\| \ . \ \|^2$ is the L_2 norm of a vector. Alarms are created by applying a threshold to the abnormality indicator vector $\boldsymbol{\psi}$. The pseudo-code for alarm generation is shown in Algorithm 1.

Algorithm 1 AMP Alarm Generation Pseudo-Code

Input: Dictionary generated from training dataset D, characteristic feature vectors $Y = \{y_1, y_2, \ldots, y_k\}$, maximum number of iterations M, threshold τ, maximum number of time windows k.
Output: Alarm
Initialization; $i \leftarrow 1$
Repeat: Find
$R_M = y_i - \sum_{i=0}^{M-1} c_i \boldsymbol{\alpha}_i$
Calculate: $\psi_i = \|R_M\|^2$
Using $\boldsymbol{D}$ and MP algorithm.
Alarm generation
if $\psi_i \leq \tau$ $alarm_i = 0$ **else** $alarm_i = 1$
Until: $i = k$

The abnormality indicator vectors are evaluated differently according to the dictionary type. If the anomaly dictionary is utilized, the abnormality value is expected to increase under attack. Similarly, when the misuse dictionary is utilized, the abnormality indicator value is expected to decrease under attack. The same approach is accurate for misuse dictionary and legitimate traffic. Since the K-SVD algorithm generates dictionaries that give minimum residual norm with a maximum number of non-zero elements, this behavior is expected as a result of the objective function of the K-SVD algorithm.

The histograms of abnormality indicator vectors obtained for CAIDA datasets using misuse and anomaly dictionaries are shown in Figure 4. It can be seen from Figure 4 that the distribution of abnormality vectors obtained from the misuse dictionary has higher values for attack-free data when compared to attack data.

D. HYBRID DETECTION FRAMEWORK WITH AMP

Using the AMP method, it is possible to generate dictionaries to perform anomaly and misuse detection. We obtain

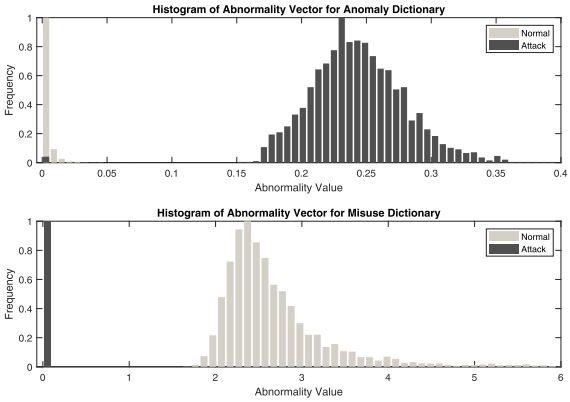

FIGURE 4. Normalized histograms of abnormality vectors obtained using anomaly and misuse dictionaries for the CAIDA dataset in the AMP method.

abnormality indicator values using the MP algorithm for each dictionary. Combining the abnormality vectors obtained from different dictionaries with a decision module, we obtain a hybrid detection framework. Additionally, the hybrid detection framework can detect together to achieve multi-class detection. In this section, we propose a hybrid detection framework that can identify multiple traffic classes simultaneously by combining the AMP method with a decision module. The proposed framework combines anomaly and misuse method to obtain a hybrid intrusion detection.

1) DECISION MODULE

In this work, the ANN is employed as the decision mechanism. ANN is the combination of a large number of interconnected processing elements (nodes) that demonstrate the ability to learn and classify data using the information in the training patterns of data. ANN is a supervised classification algorithm and requires training. The ANN topology used in decision module is shown in Figure 6.

Training the ANN includes adjusting the values of the weights and biases of the network to optimize network performance. We use feedforward ANN and mean squared error as the performance function.

$$e_{mse} = \frac{1}{N}\sum_{i=1}^{N}(t_i - a_i)^2 \tag{21}$$

The transfer function used in neural network is Hyperbolic Tangent Sigmoid Transfer Function and calculated as:

$$t(x) = \frac{2}{1 + exp(-2^x)} - 1 \tag{22}$$

where a is the output of the neural network, N is the sample size, and the t are the target outputs.

The ANN used in this work has 20 nodes in the hidden layer and 3 neurons for the output layer used in three traffic class and 2 neurons for the output layer used in two traffic classes detection.

The ANN topology used in the decision module is approximately the same with different approaches. The number of inputs of the ANN differs according to the utilized detection method. MPMP and Wavelet approach generated 16 inputs to the decision module, corresponding MPMP, and *En* of 16 feature vectors.

The AMP method generates one abnormality indicator value for each dictionary. So for the dataset that includes 2 traffic classes, the AMP method generates 2 abnormality indicator vectors. Similarly, the AMP method generates 3 abnormality indicator vectors. As a result, two inputs in 2 traffic class cases and 3 inputs for three traffic class cases are used for ANN.

2) HYBRID DETECTION FRAMEWORK TRAINING AND ALARM GENERATION

The overall hybrid detection system with the AMP, MPMP, and Wavelet methods are shown in Figure 5. The decision module generates alarms using abnormality values generated by the AMP, MPMP, and Wavelet methods.

The hybrid detection framework using the AMP method requires to be trained using a training dataset. The training has two phases corresponding to dictionary generation and training of the ANN in the decision module as seen in Figure 7. Initially, a separate dictionary is generated for each network class. The decision module is trained using the abnormality indicator vectors obtained from the training data.

For every time window, an abnormality indicator value is calculated using dictionaries corresponding to each network class in the alarm generation phase. The decision module generates alarms using the abnormality indicator values using the trained ANN.

3) HYBRID DETECTION METHOD USING WAVELET AND MPMP

In this section, we describe the usage of MPMP and Wavelet methods with the decision module. As we mentioned before, we use ANN in the decision module. In the case of MPMP and Wavelet approaches, similar to the AMP method, the framework calculates abnormality values defined in Equations (16) and (18) and generate alarms using them with decision module.

The MPMP value calculated for each attribute vector is used to train the ANN network. Also, they are fed into ANN to generate alarms in the test dataset.

Similarly, for Wavelet, the energy difference *En* between the different layers of attribute vectors, shown in the equation (18) are used to train the ANN network.

We do not build models from the training dataset in MPMP, and Wavelet approaches. However, the ANN in the decision module learns about the normal and attack behaviors of these approaches. Therefore the resulting framework will be called a hybrid detection framework using Wavelet and MPMP.

V. EVALUATION

In this section, three methods mentioned in this study were evaluated using two data sets. MPMP and Wavelet methods handle one-dimensional attribute vectors each time.

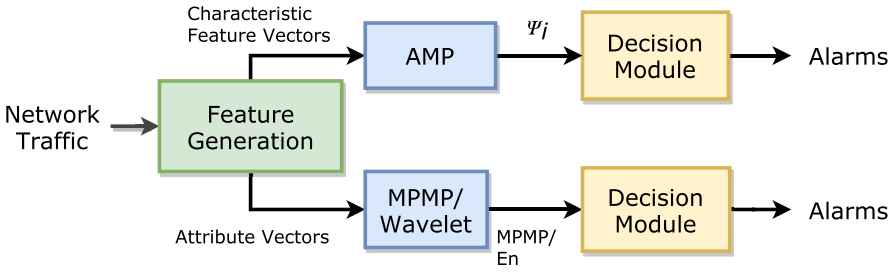

FIGURE 5. Block diagram of AMP-based Hybrid DDoS detection framework, MPMP, and Wavelet methods with decision module.

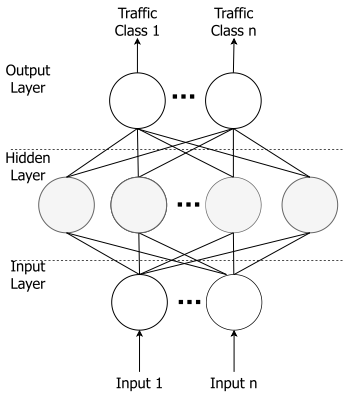

FIGURE 6. Artificial Neural Network structure used as a decision module. The number of input layer changes depending on the detection method. The number of output layer changes depending on the number of traffic classes to be detected.

TABLE 3. Confusion matrix for AMP, MPMP and Wavelet based DDoS detection for CAIDA dataset.

Method	CID	TPR (%)	FPR (%)	AUC	Acc (%)
Wavelet	0.98	99.75	0.04	0.99	99.89
MPMP	0.98	99.75	0.04	0.99	99.98
Misuse AMP	1	100	0	1	100
Anomaly AMP	0.98	99.66	0	0.99	99.89

TABLE 4. Confusion matrix for AMP, MPMP and Wavelet based DDoS detection for BOUN TCP SYN flood dataset.

Method	CID	TPR (%)	FPR (%)	AUC	Acc (%)
Wavelet	0.84	93.26	0.28	0.98	98.39
MPMP	0.96	98.91	0.01	0.99	99.78
Misuse AMP	0.95	99.47	0.46	1	99.49
Anomaly AMP	0.96	99.09	0.17	1	99.69

As a result, the anomaly indicator value is calculated for 16 different attribute vectors. In evaluation, only the result obtained for the attribute that gives the highest CID value is included in the result tables.

A. ALGORITHM COMPLEXITY ANALYSIS

The complexity analysis of the proposed algorithms is divided into two phases as training and detection.

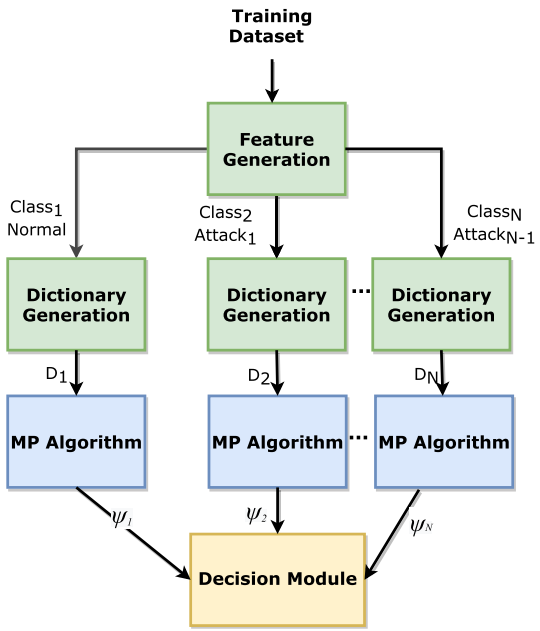

FIGURE 7. Training Hybrid DDoS detection framework based on the AMP method for multiple traffic classes.

TABLE 5. Confusion matrix for AMP, MPMP and Wavelet based DDoS detection for BOUN UDP flood dataset.

Method	CID	TPR (%)	FPR (%)	AUC	Acc (%)
Wavelet	0.896	95.532	0.052	0.982	99.088
MPMP	0.947	97.872	0.001	0.995	99.585
Misuse AMP	0.924	99.110	0.667	0.998	99.152
Anomaly AMP	0.958	99.778	0.407	0.999	99.628

We compare three different approaches in terms of computational complexity.

The AMP training phase includes dictionary generation and training of ANN. The complexity of K-SVD algorithm is $O(NM^2K)$ [51] for dictionary $D \in \mathbb{R}^{(MxN)}$, using N number of data vectors. There is no training phase in the Wavelet approach. For the MPMP method, we need to calculate the MPMP of attack-free samples of the training dataset.

We can calculate the complexity of ANN using the number of operations between neurons. We have an ANN with

TABLE 6. Comparison of AMP, MPMP and Wavelet based hybrid DDoS detection framework for two traffic classes using BOUN UDP and TCP SYN flood datasets.

Method	Dataset	CID	TPR(%)	FPR(%)	AUC	Acc
AMP	TCP SYN Flood	**0.983**	99.658	0.055	1.000	0.999
	UDP Flood	**0.980**	99.556	0.051	0.999	0.999
MPMP	TCP SYN Flood	0.946	97.826	0.000	0.990	0.990
	UDP Flood	0.971	98.936	0.000	0.995	0.990
Wavelet	TCP SYN Flood	0.680	80.926	0.000	0.907	0.953
	UDP Flood	0.688	81.455	0.011	0.912	0.957

one hidden layer. The time complexity for training a neural network with 3 layers with respectively i, j, and k nodes, with n data samples. The computational complexity of the ANN is $O(n(ij + jk.))$. The values n, j, k are the same for the MPMP, Wavelet, and AMP methods.

As a result, complexities can be compared using the difference between input neurons. The number of inputs i is equal to the number of dictionaries of the AMP method. This number equals 3 for three traffic classes and 2 for two traffic classes. In the case of the Wavelet and MPMP methods, the number of inputs depends on the number of traffic attributes shown in Table 2. As a result, $i = 16$ for two and three traffic classes.

The AMP method produces less input for ANN. Hence the complexity is reduced compared to the MPMP and Wavelet methods.

B. EVALUATION FOR TWO TRAFFIC CLASSES

The results obtained using CAIDA datasets are shown in Table 3. The CAIDA dataset includes two separate datasets containing normal and attack traffic. As a result, we obtain nearly perfect detection scores for these datasets. Because of a lower false-positive rate, AMP DDoS detection has a higher CID value. Detection using a misuse dictionary provides perfect detection, and detection using anomaly dictionary provides %99.6698 TPR with zero FPR. The Wavelet and MPMP based detection use one-dimensional traffic attribute vectors. As a result of this, we obtain 16 different results using these methods. Only the best detection performance achieved upon 16 results is included in the Tables 3, 4, and 5.

It is not a surprise to achieve perfect detection for CAIDA datasets since its a combination of two different datasets, including an attack-free dataset and a DDoS dataset. BOUN DDoS datasets are used to achieve a better comparison of the methods of this work.

The comparative results for the TCP and UDP dataset are shown in Table 4 and Table 5. The results given for MPMP and Wavelet methods are obtained using the attribute vector, which gives the highest CID value among 16 attribute vectors. For the simplicity of this paper, we did not provide the results for all feature vectors for comparison. The following inferences should be considered when evaluating these tables:

- In the evaluation of the MPMP approach, the number of unique hosts provides the highest CID (0.96) value for the TCP SYN flood attack. The second highest CID is 0.92, and it is obtained using the TCP SYN packets attribute. For other attribute vectors, an average CID of 0.17 is obtained. This average value indicates that other attribute vectors do not provide proper detection using the MPMP method.
- Similarly, the number of unique hosts provides the highest CID (0.95) value for the BOUN UDP flood dataset using the MPMP method. The closest CID is the unique flows attribute with a CID value of 0.85. For other feature vectors, we get an average CID 0.25, which indicates that other feature vectors do not provide good detection by the MPMP method.
- The conditions mentioned in the above two phrases also applies to the Wavelet method. It can be concluded that Wavelet and MPMP methods are not efficient unless the right attribute is selected.
- The AMP method achieved a higher TPR than the other two methods, even by modeling only attack-free traffic in the data set, without the need for attribute selection.

C. EVALUATION OF HYBRID AMP FRAMEWORK

The proposed framework is evaluated separately using two and three traffic classes. Similar to previous sections, the dataset is divided into training and test sets, which include %30, and %70 of the network traffic.

The two traffic classes include attack and attack free traffic while three traffic classes include two attacks. In two class evaluation, we discuss the detection of TCP and UDP attacks separately.

Because there is no publicly available DDoS dataset that contains more than one type of flood attack, we use the BOUN dataset is for three traffic class cases.

Initially, the hybrid detection framework is applied separately for BOUN UDP flood and BOUN TCP SYN flood data sets for two traffic class case Table 6. The TCP and UDP flood datasets are combined to obtain traffic that contains more multiple attack classes.

The AMP, MPMP, and Wavelet methods are used with Neural Network decision mechanism; the AMP-based framework provides better results with higher CID and TPR rates.

In Wavelet and MPMP methods, alarms are generated using abnormality vectors produced from all attribute vectors. As mentioned in previous sections, we cannot achieve discriminative abnormality vectors from all attribute vectors

TABLE 7. A comparison of hybrid detection framework based on AMP, MPMP and Wavelet using three traffic classes dataset.

Method	Class	CID	TPR (%)	FPR (%)	AUC	Acc (%)
AMP	TCP Flood	**0.97**	99.93	0.62	1.00	99.83
	UDP Flood	**0.98**	99.32	0.01	1.00	99.92
	Normal	**0.97**	99.22	0.06	1.00	99.87
Wavelet	TCP Flood	0.68	99.99	18.99	0.90	95.52
	UDP Flood	0.71	80.74	0.00	0.91	97.75
	Normal	0.71	81.27	0.00	0.90	97.77
MPMP	TCP Flood	0.94	99.98	2.69	0.99	99.46
	UDP Flood	0.95	97.83	0.00	1.00	99.79
	Normal	0.94	97.87	0.12	1.00	99.68

using Wavelet and MPMP approaches. That is the main reason we obtained lower evaluation metrics from the Wavelet approach.

The TCP and UDP flood datasets are combined to obtain traffic that contains more multiple attack classes.

When traffic data has more than two attack classes, the AMP-based hybrid framework performs better than MPMP and Wavelet-based methods, as seen in Table 7. AMP-based framework achieves higher than 0.97 CID value for all attack and attack-free classes. Although the MPMP method has high-performance metrics, it still gives lower CID and TPR for UDP flood and attack-free classes. Also, MPMP gives higher FPR for TCP SYN flood attacks. The AMP-based method works better even in cases where traffic types are not known, and only normal traffic is modeled.

VI. CONCLUSION

In this study, we propose the AMP method for DDoS detection that uses the MP algorithm. We also introduce the characteristic feature vector generated from a combination of multiple one-dimensional traffic attributes. Furthermore, in this study, adaptation to the traffic data to the MP algorithm is provided by creating dictionaries from the training dataset.

Because there is no recent study that uses the MP algorithm in the detection of DDoS attacks, the proposed methodology is compared with the MPMP and Wavelet methods. We practice these methods using CAIDA and BOUN datasets. The experimental results show that the AMP method performs better with higher CID values comparing with the Wavelet and the MPMP approaches.

Additionally, in this study, a hybrid intrusion detection framework is proposed that combines the abnormality indicator values obtained from different dictionaries. The abnormality indicator values are combined with an intelligent decision mechanism that uses ANN. MPMP and Wavelet methods are designed for only anomaly detection. We also include these methods in our Hybrid framework by combining them with the decision module utilizing the abnormality indicator vectors obtained for each traffic attribute vector.

Evaluation results show that the hybrid detection framework using the AMP approach performs better than MPMP and Wavelet-based methods for all traffic classes, including attack-free traffic class.

CONFLICT OF INTEREST

No potential conflict of interest is declared.

REFERENCES

[1] J. David and C. Thomas, "Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic," *Comput. Secur.*, vol. 82, pp. 284–295, May 2019.
[2] (2020). *Worldwide Infrastructure Security Report*. [Online]. Available: https://www.netscout.com/report/
[3] (2019). *State of the Internet, Security: 2019—A year in Review*. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-a-year-in-review-report-2019.pdf
[4] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS attack & its effect in cloud environment," *Procedia Comput. Sci.*, vol. 49, pp. 202–210, 2015.
[5] B. B. Zarpelão, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017.
[6] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert Syst. Appl.*, vol. 29, no. 4, pp. 713–722, Nov. 2005.
[7] (2007). *The Caida Ucsd 'Ddos Attack 2007' Dataset*. [Online]. Available: http://www.caida.org/data/passive/ddos-20070804_dataset.xml
[8] (2008). *The Caida Ucsd Anonymized Internet Traces 2008*. [Online]. Available: http://www.caida.org/data/passive/passive_2008_dataset.xml
[9] D. Erhan. (2019). *Boğaziçi University Ddos Dataset*. [Online]. Available: http://dx.doi.org/10.21227/45m9-9p82
[10] L. Cohen, "Time-frequency distributions–A review," *Proc. IEEE*, vol. 77, no. 7, pp. 941–981, Jul. 1989.
[11] D. Erhan, E. Anarim, and G. K. Kurt, "DDoS attack detection using matching pursuit algorithm," in *Proc. 24th Signal Process. Commun. Appl. Conf. (SIU)*, May 2016, pp. 1081–1084.
[12] Ł. Saganowski, M. Choras, R. Renk, and W. Hołubowicz, "Signal-based approach to anomaly detection in IDS systems," *Int. J. Intell. Eng. Syst.*, vol. 1, no. 4, pp. 18–24, Dec. 2009.
[13] Ł. Saganowski, M. Choras, R. Renk, and W. Hołubowicz, "A novel signal-based approach to anomaly detection in IDS systems," in *Proc. Int. Conf. Adapt. Natural Comput. Algorithms*. Springer, 2009, pp. 527–536.
[14] T. Andrysiak and Ł. Saganowski, "Anomaly detection system based on sparse signal representation," *Image Process. Commun.*, vol. 16, nos. 3–4, pp. 37–44, Jan. 2011.
[15] M. Choraś, Ł. Saganowski, R. Renk, and W. Hołubowicz, "Statistical and signal-based network traffic recognition for anomaly detection," *Expert Syst.*, vol. 29, no. 3, pp. 232–245, Jul. 2012.
[16] R. Renk, L. Saganowski, W. Holubowicz, and M. Choras, "Intrusion detection system based on matching pursuit," in *Proc. 1st Int. Conf. Intell. Netw. Intell. Syst.*, Nov. 2008, pp. 213–216.
[17] B. Eriksson, P. Barford, R. Bowden, N. Duffield, J. Sommers, and M. Roughan, "BasisDetect: A model-based network event detection framework," in *Proc. 10th Annu. Conf. Internet Meas. (IMC)*, 2010, pp. 451–464.
[18] H. Xia, B. Fang, M. Roughan, K. Cho, and P. Tune, "A BasisEvolution framework for network traffic anomaly detection," *Comput. Netw.*, vol. 135, pp. 15–31, Apr. 2018.

[19] T. Andrysiak, Ł. Saganowski, and M. Choraś, "DDoS attacks detection by means of greedy algorithms," in *Image Processing and Communications Challenges*. Springer, 2013, pp. 303–310.
[20] V. M. Patel and R. Chellappa, "Dictionary-based methods for object recognition*," in *Handbook of Statistics*, vol. 31. Amsterdam, The Netherlands: Elsevier, 2013, pp. 203–225.
[21] M. Aharon, M. Elad, and A. Bruckstein, "*K*-SVD: An algorithm for designing overcomplete dictionaries for sparse representation," *IEEE Trans. Signal Process.*, vol. 54, no. 11, pp. 4311–4322, Nov. 2006.
[22] S. D. Bay, D. Kibler, M. J. Pazzani, and P. Smyth, "The UCI KDD archive of large data sets for data mining research and experimentation," *ACM SIGKDD Explor. Newslett.*, vol. 2, no. 2, pp. 81–85, Dec. 2000.
[23] R. Fontugne, P. Borgnat, P. Abry, and K. Fukuda, "MAWILab: Combining diverse anomaly detectors for automated anomaly labeling and performance benchmarking," in *Proc. 6th Int. Conf. (Co-NEXT)*, 2010, pp. 1–12.
[24] *Intrusion Detection Evaluation Dataset*, M DARPA, Arlington County, VA, USA, 2000.
[25] C. C. Ateş, S. Özdel, and E. Anarım, "Graph–based anomaly detection using fuzzy clustering," in *Proc. Int. Conf. Intell. Fuzzy Syst.* Springer, 2019, pp. 338–345.
[26] C. Ates, S. Ozdel, and E. Anarim, "Clustering based DDoS attack detection using the relationship between packet headers," in *Proc. Innov. Intell. Syst. Appl. Conf. (ASYU)*, Oct. 2019, pp. 1–6.
[27] C. Ates, S. Ozdel, and E. Anarim, "A new network anomaly detection method based on header information using greedy algorithm," in *Proc. 6th Int. Conf. Control, Decis. Inf. Technol. (CoDIT)*, Apr. 2019, pp. 657–662.
[28] C. Ates, S. Ozdel, M. Yildirim, and E. Anarim, "Network anomaly detection using header information with greedy algorithm," in *Proc. 27th Signal Process. Commun. Appl. Conf. (SIU)*, Apr. 2019, pp. 1–4.
[29] C. Ates, S. Ozdel, M. Yildirim, and E. Anarim, "DDoS attack detection using greedy algorithm and frequency modulation," in *Proc. 27th Signal Process. Commun. Appl. Conf. (SIU)*, Apr. 2019, pp. 1–4.
[30] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skorić, "Measuring intrusion detection capability: An information-theoretic approach," in *Proc. ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*. New York, NY, USA: ACM, 2006, pp. 90–101.
[31] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2012.
[32] E. Adi, Z. Baig, and P. Hingston, "Stealthy denial of service (DoS) attack modelling and detection for HTTP/2 services," *J. Netw. Comput. Appl.*, vol. 91, pp. 1–13, Aug. 2017.
[33] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2015, pp. 77–81.
[34] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, "Booters—An analysis of DDoS-as-a-service attacks," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 243–251.
[35] D. Erhan, E. Anarim, G. K. Kurt, and R. Kosar, "Effect of DDoS attacks on traffic features," in *Proc. 21st Signal Process. Commun. Appl. Conf. (SIU)*, Apr. 2013, pp. 1–4.
[36] T. T. Oo and T. Phyu, "A statistical approach to classify and identify DDoS attacks using UCLA dataset," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 2, no. 5, pp. 1766–1770, 2013.
[37] B. Wang, Z. Li, D. Li, F. Liu, and H. Chen, "Modeling connections behavior for Web-based bots detection," in *Proc. 2nd Int. Conf. E-Bus. Inf. Syst. Secur.*, May 2010, pp. 1–4.
[38] S. M. Tabatabaie Nezhad, M. Nazari, and E. A. Gharavol, "A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 700–703, Apr. 2016.
[39] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," in *Proc. 6th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2014, pp. 63–68.
[40] P. K. Singh, S. Kumar Jha, S. K. Nandi, and S. Nandi, "ML-based approach to detect DDoS attack in V2I communication under SDN architecture," in *Proc. IEEE Region 10 Conf. (TENCON)*, Oct. 2018, pp. 0144–0149.
[41] W. Lu and A. A. Ghorbani, "Network anomaly detection based on wavelet analysis," *EURASIP J. Adv. Signal Process.*, vol. 2009, no. 1, p. 4, Dec. 2008.
[42] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2016, pp. 258–263.
[43] O. Boyar, M. E. Ozen, and B. Metin, "Detection of denial-of-service attacks with SNMP/RMON," in *Proc. IEEE 22nd Int. Conf. Intell. Eng. Syst. (INES)*, Jun. 2018, pp. 000437–000440.
[44] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Netw.*, vol. 44, no. 5, pp. 643–666, Apr. 2004.
[45] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 310–317.
[46] D. Jankowski and M. Amanowicz, "Intrusion detection in software defined networks with self-organized maps," *J. Telecommun. Inf. Technol.*, vol. 4, pp. 3–9, Dec. 2015.
[47] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," *Arabian J. Sci. Eng.*, vol. 42, no. 2, pp. 425–441, Feb. 2017.
[48] O. Osanaiye, K.-K.-R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, May 2016.
[49] A. Grossmann and J. Morlet, "Decomposition of functions into wavelets of constant shape, and related transforms," in *Mathematics+Physics: Lectures on Recent Results*, vol. 1. Singapore: World Scientific, 1985, pp. 135–165.
[50] R. Rubinstein, T. Peleg, and M. Elad, "Analysis K-SVD: A dictionary-learning algorithm for the analysis sparse model," *IEEE Trans. Signal Process.*, vol. 61, no. 3, pp. 661–677, Feb. 2013.
[51] E. M. Eksioglu and O. Bayir, "K-SVD meets transform learning: Transform K-SVD," *IEEE Signal Process. Lett.*, vol. 21, no. 3, pp. 347–351, Mar. 2014.

DERYA ERHAN (Member, IEEE) received the B.Sc. degree from Hacettepe University, Ankara, Turkey, in 2002, and the M.Sc. degree from Boğaziçi University, İstanbul, Turkey, in 2007, where she is currently pursuing the Ph.D. degree with the Electrical and Electronics Engineering Department.

From 2003 to 2008, she worked as a Senior Telecom Specialist at the Türk Telekom Network Operations Department and the Information Security Department, Turkey. From 2008 to 2020, she worked at the Information Technology Department, Boğaziçi University, as a Network Administrator, an Assistant Manager, and the Manager. Her research interests include anomaly detection, intrusion detection, and network-based detection methods.

EMİN ANARIM received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electronic and electrical engineering from Boğaziçi University, İstanbul, Turkey, in 1981, 1983, and 1985, respectively.

He is currently a Professor with the Electrical and Electronics Engineering Department, Boğaziçi University. He is also an Adjunct Professor with The George Washington University. He has given several courses to industry and government institutions on signal processing, video coding, secure telecommunications, mobile communications, lawful interception techniques in telecommunications, cryptographic techniques, and network security. He has frequently acted as a Consultant for various telecommunications companies in Turkey. He has published more than 190 papers carrying his name have appeared in various journals and conference proceedings. His current research interests include multimedia wireless communications, information, and network security.