SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9:**2032–2041
Published online 22 February 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1460

RESEARCH ARTICLE

FFSc: a novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis

Nazrul Hoque[1], Dhruba K. Bhattacharyya[1]* and Jugal K. Kalita[2]

[1] Department of Computer Science and Engineering, Tezpur University, Sonitpur, Assam, India
[2] Department of Computer Science, University of Colorado, Colorado Springs, CO, U.S.A.

ABSTRACT

A Distributed Denial of Service (DDoS) attack is a major security threat for networks and Internet services. Attackers can generate attack traffic similar to normal network traffic using sophisticated attacking tools. In such a situation, many intrusion detection systems fail to identify DDoS attack in real time. However, DDoS attack traffic behaves differently from legitimate network traffic in terms of traffic features. Statistical properties of various features can be analyzed to distinguish the attack traffic from legitimate traffic. In this paper, we introduce a statistical measure called Feature Feature score for multivariate data analysis to distinguish DDoS attack traffic from normal traffic. We extract three basic parameters of network traffic, namely, entropy of source IPs, variation of source IPs, and packet rate to analyze the behavior of network traffic for attack detection. The method is validated using CAIDA DDoS 2007 and MIT DARPA datasets. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS
DDoS; correlation; low-rate attack; feature

***Correspondence**
Dhruba K. Bhattacharyya, Department of Computer Science and Engineering, Tezpur University, Sonitpur, Assam, India.
E-mail: dkb@tezu.ernet.in

1. INTRODUCTION

Distributed Denial of Service (DDoS) attack is a major security threat for network security researchers and practitioners. The complexity and frequency of occurrence of DDoS attacks are growing in parallel with rapid developments of the Internet and associated computer networks. A significant number of network security tools are available on the Internet to generate network attacks as well as to defend and analyze network attacks [1]. Attackers can generate attack traffic similar to normal network traffic so that an anomaly detection system cannot detect any significant difference between the two. A distributed denial of service attack is generated in a coordinated manner using a large number of compromised machines. An attacker may be able to disrupt a service on a server immediately or it can consume resources of the server reducing services for legitimate users. A DDoS attack can be generated using botnets, and a botnet may have a few hundred to a few thousands or even millions of bots. Therefore, DDoS attack intensity may vary from moderate to very high and may cause huge damage and financial loss to organizations.[†]

For example, on 11 February 2014, a new massive DDoS attack was launched by hackers on the anti-DDoS protection firm CloudFlare, reaching more than 400 Gbps at its peak of traffic.[‡] Arbor 10th Annual Worldwide Infrastructure Security Report claims that over one third of data center operators saw DDoS attacks, which exhausted their Internet bandwidth in 2015. Thus, DDoS attack is a major security issue for data center operators.

Network intrusion detection systems fall into two categories, namely, misuse detection and anomaly detection. Misuse detection, also referred to as signature-based detection, detects only known attacks if the traffic pattern matches already created attack signatures. On the other hand, anomaly detection generates a profile for the normal network traffic and if the observed network traffic profile deviates from the normal profile significantly, the traffic is marked anomalous. People use a variety of methods such as statistical, soft computing, data mining, and machine learning to generate normal profile for network traffic analysis [2,3]. In statistical approaches, class discriminant features are analyzed using different techniques

[†] http://www.arbornetworks.com/.

[‡] http://thehackernews.com/2014/02/NTP-Distributed-Denial-of-Service-DDoS-attack.html.

to learn the behavior of network traffic. However, many correlation-based statistical methods cannot differentiate attack traffic from the normal. This is because a sophisticated attacker may generate attack traffic very similar to normal network traffic to evade detection. In this paper, we use multivariate data analysis to analyze traffic behavior. In our approach, we distribute the change of one feature to other features, reflecting the change of the whole object.

1.1. Motivation

It is very common to use statistical measures such as mutual information, entropy, principal components analysis, and similarity or distance measures to detect anomalous patterns in network traffic. During network traffic analysis, statistical analysis of individual traffic parameters or attributes often misleads anomaly detection and hence raises a large number of false alarms. In addition, the attacker always tries to evade the detection mechanism by generating attack traffic similar to the normal traffic.

Correlation measures, such as Pearson, Spearman, and Kendall correlation sometimes produce high correlation values between two objects even though they are very dissimilar. Because of the shifting or scaling or shifting-and-scaling correlation [4] among features, these correlation measures are sometimes inadequate in analyzing data object for pattern classification. For example, let us assume that all parameter values except one or two for normal network flows are almost the same as the parameter values for attack flows. If Pearson, Spearman, or Kendall's correlation measures are used, they fail to identify such a small deviation. So to detect mild but still significant deviations in a feature with reference to other parameters of an object, multivariate data analysis is useful.

1.2. Contribution

The major contributions of this paper is listed below.

(1) We introduce an effective measure called Dis-HBK to estimate the difference between attack traffic and legitimate traffic.
(2) We present a DDoS defense method that uses FFSc and multivariate data analysis for detection of DDoS attack.
(3) Another measure called AI_HBK is introduced to classify low-rate and high-rate DDoS attacks.
(4) The method is dependent on a small set of network traffic parameters for attack detection and the performance of the method is validated on two network security datasets.

1.3. Paper organization

The remainder of this paper is organized as follows.

We survey the related work in Section 2. A few definitions and the problem of DDoS attack detection in terms of correlation measures is defined in Section 3. The proposed method for DDoS attack detection is presented in Section 4. The experimental evaluation of the implemented method is discussed in Section 5, followed by our conclusions in Section 6.

2. RELATED WORK

Several statistical methods have been used in the past for DDoS attack detection. Feinstein *et al.* [5] discuss different statistical metrics such as entropy, distributions of packet attributes, and chi-square statistics to identify DDoS attacks. The authors also describe a DDoS detection-response prototype to extend the detection mechanism for an effective response decision. A covariance analysis model for DDoS attack detection is proposed by Jin *et al.* [6]. The method is very effective in detecting SYN flooding DDoS attacks as well as attacks that are subtle changes from normal behaviors. A novel proactive method for bandwidth DDoS attack detection using sequential nonparametric change points is proposed by Peng *et al.* [7]. The method uses IP addresses to analyze network traffic to detect bandwidth attacks. It monitors incoming network traffic and computes the arrival rate of new source IP addresses. The main advantage of this method is that it can detect DDoS attacks close to the sources at an early stage. Xiang *et al.* [8] proposed a low-rate DDoS attack detection and traceback method using two new and effective information metrics for low-rate DDoS attacks detection, namely, generalized entropy and information distance metric. The method detects low-rate attack by adjusting the value of order α of the generalized entropy and information distance metrics. The proposed entropy-based distance method increases the gap between attack traffic and normal traffic and as a result the method effectively detects low-rate DDoS attacks.

3. DEFINITIONS AND PROBLEM SETTING

The following definitions helps in describing our scheme.

Definition 1. *Feature Feature ordered Relation (FFoR): FFoR of a feature f_i with all other features f_j of an object O_i is defined using Equation (1).*

$$FFoR\left(O_i^{f_i}\right) = \sum_{j=1\&i\neq j}^{n} (|f_i - f_j|) \tag{1}$$

where $1 \leq i \leq n$.

Definition 2. *Average FFoR (AFFoR): We define AFFoR of an object O_i as the mean value of its individual FFoR values and it can be expressed using Equation (2).*

$$AFFoR(O_i) = \frac{\sum_{j=1}^{n} \left(FFoR\left(O_i^{f_j}\right)\right)}{n} \quad (2)$$

Definition 3. *The Deviation vector (Dev): Deviation vector of an object O_i can be defined as the absolute difference between the FFoR values of the object and its corresponding AFFoR value. The Dev of a feature f_j is computed using Equation (3).*

$$Dev\left(O_i^{f_j}\right) = |AFFoR(O_i) - FFoR\left(O_i^{f_j}\right)|, \forall j = 1, 2, \cdots n \quad (3)$$

Definition 4. *FF-score (FFSc): We define FFSc of an object O_i as the degree of similarity in terms of its Dev and mean value, which is given by the Equation (4).*

$$FFSc(O_i) = \frac{\left(O_i \times Dev(O_i)^{\mathsf{T}}\right)}{(mean(O_i) + mean(Dev(O_i)))} \quad (4)$$

where $Dev(O_i)^{\mathsf{T}}$ represents the transpose of Dev and $mean(O_i)$ represents the mean of all the feature values of the object O_i. The Deviation vector reflects changes among the feature values of an object. Attack traffic will certainly have unpredictable values at least for one or more feature(s). However, normal network traffic parameters follow a specific pattern. So, the FFSc value among the features will reflect a close relation, whereas in an attack situation, network traffic parameters will follow diverse relations among features. Using the deviation vector of an object O_i, we compute an FFSc value for every object. The score is compared with discriminate DDoS attack traffic from normal traffic.

3.1. An example of computing Feature Feature score value

Let us consider three objects, O_1, O_2, and O_3 with five features as given in the following:

O_1=[5, 12, 9, 11, 18], O_2=[13, 7, 21, 3, 6] and O_3=[25, 20, 17, 15,11]

Step 1: Compute FFoR value for object O_1 for every feature f_1,f_2,f_3,f_4,f_5 using Definition (1).
$f_1 = |5 - 12| + |5 - 9| + |5 - 11| + |5 - 18| = 30$
$f_2 = |12 - 5| + |12 - 9| + |12 - 11| + |12 - 18| = 17$
$f_3 = |9 - 5| + |9 - 12| + |9 - 11| + |9 - 18| = 18$
$f_4 = |11 - 5| + |11 - 12| + |11 - 9| + |11 - 18| = 16$
$f_5 = |18 - 5| + |18 - 12| + |18 - 9| + |18 - 11| = 35$
$FFoR(O_1) = [30, 17, 18, 16, 35]$

Step 2: Compute AFFoR for object O_1 using Definition (2).
$AFFoR(O_1) = (30 + 17 + 18 + 16 + 35)/5 = 23.20$

Step 3: Compute Dev for object O_1 from the AFFoR using Definition (3).
For feature f_1 = |30 – 23.20| = 6.8
For feature f_2 = |17 – 23.20| = 6.2
For feature f_3 = |18 – 23.20| = 5.2
For feature f_4 = |16 – 23.20| = 7.2
For feature f_5 = |35 – 23.20| = 11.8
So, Dev(O_1)= (6.8, 6.2, 5.2, 7.2, 11.8)

Step 4: Compute FFSc for object O_1 using Definition (4).
$FFSc(O_1) = \frac{(5,12,9,11,18)\times(6.8,6.2,5.2,7.2,11.8)'}{mean(5,12,9,11,18)+mean(6.8,6.2,5.2,7.2,11.8)}$
$FFSc(O_1) = \frac{446.8}{18.44} = 24.229$
Similarly, FFSc for O_2 and O_3 can be computed.

3.2. Problem definition

Many multivariate data analysis techniques [9], such as multivariate correlation analysis, covariance, and maximum likelihood ratio, are used for network anomaly detection. These methods consider linear dependencies among various features of network traffic. A correlation value computed on two samples or objects represents the level of dependency between them. If an attack is generated from a botnet, then the attack traffic has strong correlation among its samples because the botmaster uses the same attack statistics during attack generation. Hence, a statistical method can discriminate DDoS attack traffic from normal traffic using a correlation measure. On the other hand, if the attacker generates attack traffic very similar to normal network traffic, a correlation measure may not distinguish the difference between normal and attack traffic. So, instead of computing correlation between network samples, it is possible to analyze multiple network traffic parameters for each traffic sample. Multiple network traffic features are analyzed in such a way that change in an individual feature value may reflect the overall change in the network traffic sample. Although an attacker can generate attack traffic very similar to normal network traffic, at least one attack feature will have a different value (with a small or larger difference in that feature value) during the attack period. The proposed FFSc measure is able to identify the change in an attack traffic feature during DDoS attack detection.

4. PROPOSED METHOD

In this paper, we propose a DDoS attack detection method using the FFSc measure that analyzes individual network traffic samples or objects. The method consists of two phases; (i) normal traffic analysis phase and (ii) captured traffic analysis phase. Besides these two analysis phases, the method uses a pre-processing step where relevant features are extracted from network traffic. The proposed framework of our method is shown in Figure 1. The extracted features such as entropy of source IPs, variation of source IPs, and packet rate are used during analysis phases for DDoS attack detection.

Entropy of Source IPs (E_{sip}): Entropy of source IPs for each sample traffic is calculated using Equation 5.

DOI: 10.1002/sec

$$H(X) = -\sum_{i}^{n} P(x_i) \log_2 P(x_i) \quad (5)$$

where X is a random variable representing source IPs and n is the total number of possible values for the source IP.

Variation of Source IPs (V_{sip}): Variation among source IPs is the rate of change of IP addresses w.r.t time in a traffic sample. If an IP address changes frequently, the variation will be high.

Packet rate (P_{rate}): Packet rate is total number of packets transmitted in 1 s, that is, total number of packets in a 1-s traffic sample.

In normal traffic analysis, the method samples network traffic into multiple 1 s time windows. From each sample, the method extracts three relevant features, namely, entropy of source IPs, variation of source IPs, and packet rate. The features are used to compute FFSc using Equation 4 for each sample. Based on the FFSc value of each sample object in normal network traffic, a normal profile is generated. The normal profile stores two parameters, namely, mean of FFSc, that is, M_{FFSc} and an optimal range of FFSc values called N_{range}. The optimal range of FFSc values is the difference between maximum and minimum FFSc for normal traffic. N_{range} is used to normalize the similarity (dissimilarity) value between any two traffic samples. Instead of normalizing the similarity (dissimilarity) value during similarity computation, we can normalize every feature value in a network traffic sample.

During captured traffic analysis, the method works online and captures raw network traffic. It uses the same processes that are applied during normal traffic analysis. The method computes the deviation-based FFSc score for each candidate sample captured online and compares with the pre-computed prototype mean score for normal traffic samples using Equation (6) to give a dissimilarity value, that is, Dis_HBK as given in the following.

$$Dis\_HBK = \frac{|C_{FFSc} - M_{FFSc}|}{N_{range}} \quad (6)$$

If the Dis_HBK value is greater than a user defined threshold α, an alarm is generated. The Dis_HBK value for different samples of network traffic on CAIDA and DARPA datasets is shown in Figure 2(a) and (b), respectively.

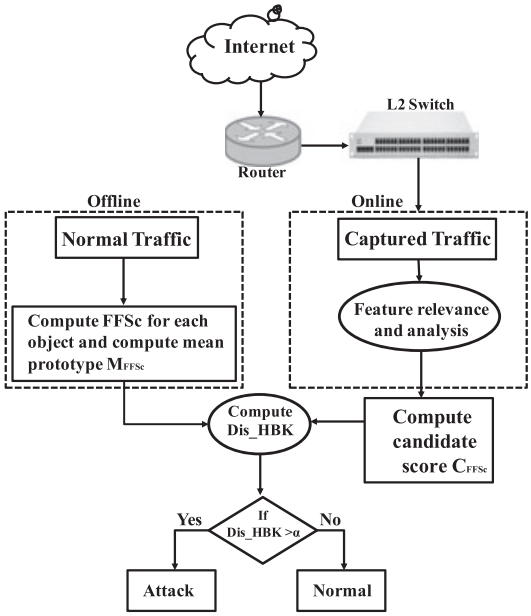


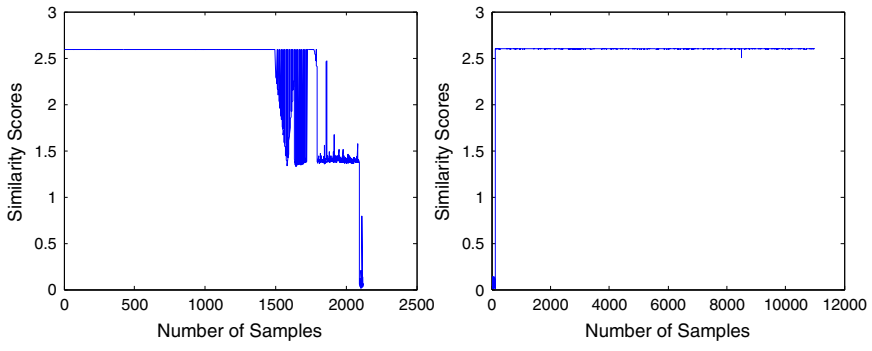
Figure 1. Framework of the proposed method.

4.1. Analysis of the proposed method

In this section, we discuss the theoretical background of the proposed DDoS detection method using FFSc. First, we establish that FFSc can distinguish DDoS attack traffic from the normal traffic. Following this foundation, the effectiveness of the proposed method is analyzed on two benchmark datasets.

In order to make our analysis clear, we make the following assumptions.

(1) DDoS attack is generated on a single victim from the same type of sources in a distributed manner.



(a) Dis_HBK values on CAIDA dataset (b) Dis_HBK values on DARPA dataset

Figure 2. Comparison of Dis_HBK values for normal and DDoS attack traffic.

(2) Normal network traffic follows specific patterns considering all attributes whereas for attack traffic, at least one attributes shows a diverging pattern.

The proposed method analyzes network traffic samples to know the behavior of different features among themselves during normal as well as attack period. We define FFSc on multiple attributes of a network traffic sample to identify the relationship among the attributes for DDoS attack detection. Let us take an example to explain the proposed method. An object O_i consists of three distinct attributes F_1, F_2, and F_3 with different values. As shown in Table I, O_1, O_2, and O_4 are attack samples, whereas others, that is, O_3 and O_5, are normal samples. In a normal environment, traffic samples follow normal behavior for which the features of the samples have close correlation among themselves. On the other hand, during flooding DDoS attacks, abrupt change occurs in at least one or more features of a network sample. A sophisticated attacker may generate an attack in such a way that all the features of a sample follow the same behavior like a normal sample except for one feature. In such a situation, many correlation-based statistical measures may not be able to discriminate an attack samples from normal samples. This situation is explained in Table II, where correlation for all pairs of samples are found 1, that is, exactly similar.

To overcome the problem discussed previously, our DDoS detection method analyzes traffic samples with reference to the normal profile. The method analyzes individual traffic samples to find relationship among the features. It uses FFoR that gives equal weight to all the features of a sample using Equation (1). The method computes a score called FFSc using Equation (4). FFSc is used to find the dissimilarity between any two samples. According to our assumption, at least one traffic feature shows divergent pattern compared with normal features. Based on this divergent pattern value, the method distinguishes the difference between normal and attack samples. FFSc is used to measure the difference of a feature with respect to others and the change of a feature is transmitted to others. Hence, the FFSc value of an attack sample will never be equal to the FFSc value of normal samples. So if an attacker generates attack traffic similar to normal traffic with identical features values for all the features except one feature, the method still distributes the difference in the feature value to all other features. We can compute a dissimilarity score between this distribution and a normal sample. The dissimilarity score is computed using Equation (6). In Table II, we show the dissimilarity score between any two traffic sample. From the dissimilarity scores, we infer that sample pairs (O_1, O_2) and (O_3, O_5) are similar where as other pairs are dissimilar.

Table I. List of five objects.

Object	F_1	F_2	F_3
O_1	365	2.52	0.9533
O_2	379	2.55	0.9709
O_3	345574	12.98	0.94
O_4	166453	12.7	0.9866
O_5	357663	12.79	0.94

Table II. Correlation values of different object pairs.

Object	PC	SC	KC	HD	JC	FFSc
O_1, O_2	1	1	1	1	1	0.0001
O_2, O_3	1	1	1	1	1	2.5409
O_3, O_1	1	1	1	1	1	1.3185
O_4, O_5	1	1	1	1	1	1.3385
O_5, O_2	1	1	1	1	1	2.5609
O_3, O_5	1	1	1	1	1	0.0200

PC, Pearson correlation; SC, Spearman correlation; KC, Kendall correlation; HD, Hamming distance; JC, Jaccard coefficient; FFSc, Feature Feature score.

4.2. Proposed algorithm

The proposed DDoS attack detection method analyzes normal traffic to generate a profile, which is used for detection. The normal profile generation module is shown in Algorithm 1.

The method analyzes captured network traffic in the detection phase. The steps of the detection module are shown in Algorithm 2.

Data: Normal network traffic samples, $S_1, S_2, \cdots S_k$
Result: M_{FFSc}, N_{range}
begin
  Extract features from normal traffic samples;
  foreach *i=1 to k* **do**
    Extract entropy of source IPs, i.e., E_{sip};
    Variation of source IPs, i.e., V_{sip};
    Packet rate, i.e., P_{rate};
    $O_i = \{E_{sip}, V_{sip}, P_{rate}\}$
  end
  foreach *object* $O_i, 1 \leq i \leq k$ **do**
    Compute FFSc using Equation (4)
  end
  Compute mean M_{FFSc} i.e., $M_{FFSc} = \frac{\sum_{i=1}^{k} FFSc(i)}{k}$;
  Find maximum and minimum FP-score values from all normal samples, i.e.,;
  Max_{FFSc}=maximum of all FFSc;
  Min_{FFSc}=minimum of all FFSc;
  $N_{range} = Max_{FFSc} - Min_{FFSc}$;
  Output: M_{FFSc} and N_{range}
end

Algorithm 1: Generate Normal Profile

4.3. Classification of low-rate and high-rate Distributed Denial of Service attack traffic

Distributed Denial of Service (DDoS) attack traffic can be classified into different attack types in terms of

DOI: 10.1002/sec

Data: Captured network traffic samples, $C_1, C_2, \cdots C_m$
Result: DDoS attack samples
begin
  Extract features from captured network traffic samples.;
  foreach *i=1 to m* **do**
    Extract entropy of source IPs i.e., E_{sip};
    Variation of source IPs i.e., V_{sip};
    Packet rate i.e., P_{rate};
    $O_i = \{E_{sip}, V_{sip}, P_{rate}\}$
  end
  foreach *object* O_i, *where* $1 \leq i \leq m$ **do**
    Compute FFSc using Equation (4);
  end
  Compare FFSc with normal profile and compute proximity using Equation 6.;
  if $Dis\_HBK > \theta$ **then**
    Attack sample;
  else
    Normal Sample;
  end
end

Algorithm 2: DDoS attack detection module

attack parameters. Based on attack rate dynamics, Mirkovic *et al.* [10] classify DDoS attacks either as high-rate or low-rate attack. The proposed method not only identifies the DDoS attack samples, but it can identify the type of attack as well. The method first identifies the DDoS attack samples using Algorithm 2 and then classifies the attack samples either as low rate or high rate. It is very difficult to identify low-rate attack traffic from the normal traffic because low-rate attack behaves very similar to normal network traffic. In this paper, we define another novel measure using four distinct network traffic parameters to classify low-rate and high-rate attacks.

A new measure called AI_HBK is used to identify low-rate and high-rate DDoS attack samples. The measure uses entropy of source IPs (E_{sip}), variation index of source IPs (V_{sip}), packet rate (P_{rate}), and distinct source IPs (D_{sip}). We introduce the second measure, that is, AI_HBK, to estimate the attack intensity using Equation (7).

$$AI\_HBK = 1 - \frac{E_{sip} * \left(\frac{P_{rate}}{D_{sip}}\right)}{\frac{D_{sip}}{V_{sip}}} \tag{7}$$

It computes attack intensity (AI_HBK) of each network traffic sample, and if the attack intensity is less than 0, then the attack type is low-rate attack otherwise the attack is high-rate attack.

Theorem 1. *The lower bound of the variation of packet rate of high-rate attack traffic is higher than the upper bound of the variation of packet rate of low-rate DDoS attack. Mathematically,* $UB^{low\_r} < LB^{high\_r}$.

Proof. We know that DDoS attacks are classified in terms of low rate and high rate based on number of attack packets generated per second. For a given DDoS attack traffic, let us assume that $UB^{low\_r} \geq LB^{high\_r}$. High-rate DDoS attack is defined in terms of higher packet rate per second (i.e., say 10 000 packets/s in CAIDA 2007) or higher attack intensity, and similarly, a low-rate DDoS attack is defined in terms of lower packet rate per second (i.e., say 1000 packets/s in CAIDA 2007) or lower attack intensity. So, a high-rate DDoS attack will be initiated with relatively higher packet rate than a low-rate attack, and hence, the lower bound or minimum of the packet rate variation of high-rate DDoS attack cannot be less than the upper bound or maximum of the packet rate variation of low-rate DDoS attack traffic. Therefore, the aforementioned assumption contradicts and hence the proof. □

Lemma 1. $AI\_HBK > 0$ *for high-rate attack.*

Proof. According to the definition of high-rate attack, the number of packets transmitted per second is always greater than 10 000. That is, $P_{rate} > 10\,000$ and the number of distinct source IPs for a high-rate attack is also very high. But, variation index is comparatively low for both high-rate and low-rate attacks. Hence, $\frac{P_{rate}}{D_{sip}}$ in Equation 7 yields a very low value, and if this value is again divided by D_{sip} (neglecting V_{sip} in the denomination of Equation 7), then it yields a value that cannot be greater than 1. So, the value of $AI\_HBK > 0$. Mathematically,

$$AI\_HBK = 1 - \frac{E_{sip} \times \left(\frac{P_{rate}}{D_{sip}}\right)}{\frac{D_{sip}}{V_{sip}}}$$

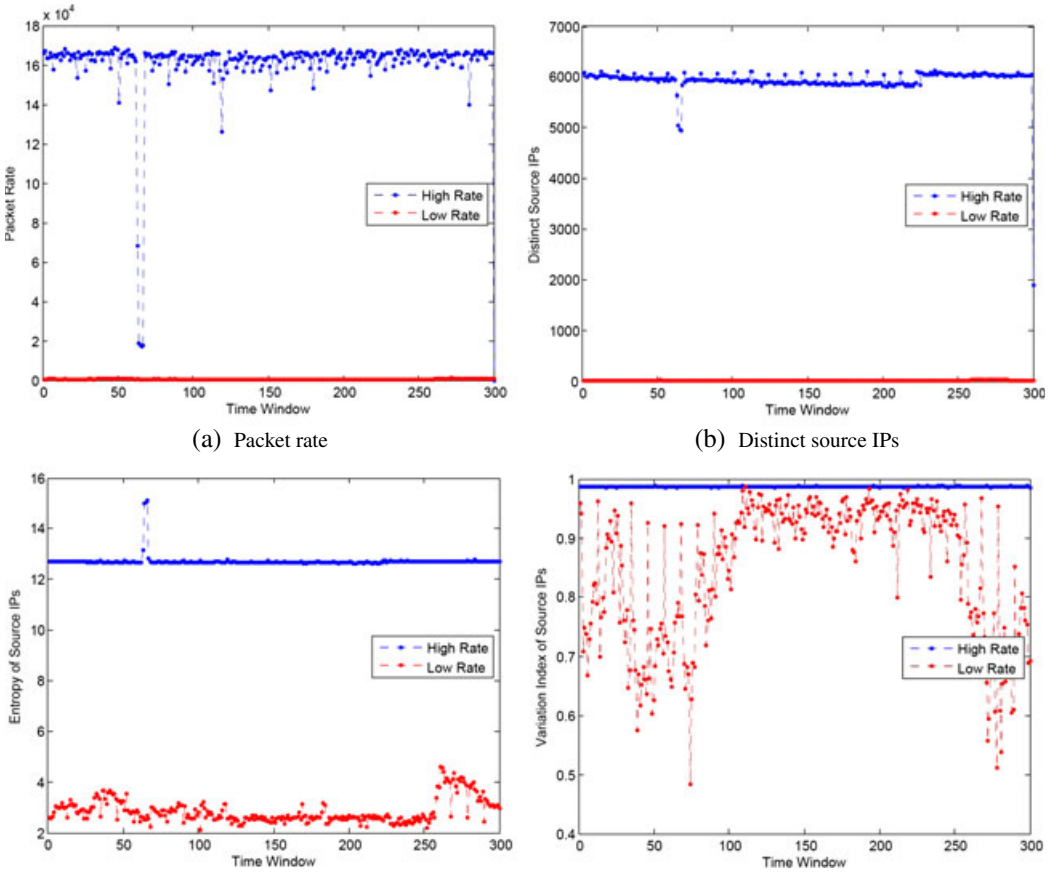
$$AI\_HBK = 1 - \frac{E_{sip} \times P_{rate} \times V_{sip}}{D_{sip}^2}$$

It is observed that $P_{rate} > D_{sip} \implies$ but $P_{rate} < D_{sip}^2$.
Because $E_{sip}, V_{sip} < D_{sip}$, hence $\frac{E_{sip} \times P_{rate} \times V_{sip}}{D_{sip}^2} << 1$.
So $AI\_HBK > 0$. □

Lemma 2. $AI\_HBK < 0$ *for low-rate attack.*

Proof. In case of low-rate attack, the number of packets transmitted per second is always less than 1000, that is, $P_{rate} < 1000$ and the number of distinct source IPs is very low (less than 10 as shown in Figure 3) compared with P_{rate}. Hence, $\frac{P_{rate}}{D_{sip}}$ in Equation 7 yields a large value (greater than 100 but less than 1000), and if this value is divided by D_{sip} (neglecting V_{sip} in he denomination of Equation 7), which is much smaller than P_{rate}, it yields a value that is always greater than 1. Hence, $AI\_HBK < 0$. Mathematically,

$$AI\_HBK = 1 - \frac{E_{sip} \times \left(\frac{P_{rate}}{D_{sip}}\right)}{\frac{D_{sip}}{V_{sip}}}$$



(a) Packet rate (b) Distinct source IPs

(c) Entropy of Source IPs (d) Variation of source IPs

Figure 3. Comparison of low-rate and high-rate attack.

$$AI\_HBK = 1 - \frac{E_{sip} \times P_{rate} \times V_{sip}}{D_{sip}^2}$$

It is observed that $P_{rate} > D_{sip}$ but $P_{rate} > D_{sip}^2$.

Because $E_{sip}, V_{sip} < D_{sip}$, hence $\frac{E_{sip} \times P_{rate} \times V_{sip}}{D_{sip}^2} > 1$.

So, $AI\_HBK < 0$. □

5. EXPERIMENTAL RESULT

In order to evaluate the effectiveness of the proposed DDoS detection method, an experiment was carried out on a workstation with 12 GB main memory, 2.26 GHz Intel Xeon processor and 64-bit Windows 7 operating system. The proposed DDoS detection framework was implemented in MATLAB 2015 software.

5.1. Experimental evaluation

To validate the detection method, we use two network intrusion datasets, namely, CAIDA DDoS 2007 [11][§] and DARPA.[¶] The performance of our method in terms of accuracy is shown in Figures 4(a) and (b) for CAIDA and DARPA datasets, respectively. We carried out the experiment in two ways, (i) normalized the data before analysis and (ii) without normalizing data during analysis but normalizing the data during similarity computation as implied in our proposed method.

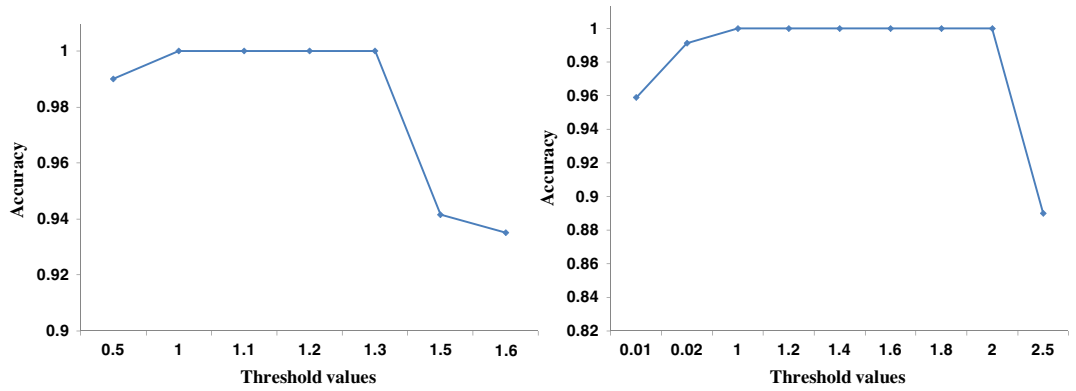
The CAIDA DDoS attack dataset is a sequence of anonymized traffic traces from a DDoS attack on 4 August 2007 (20:50:08 UTC to 21:56:16 UTC) containing approximately 1-h traffic. This type of denial-of-service attack attempts to block access to the targeted server by consuming computing resources on the server and by consuming all of the bandwidth of the network connecting the server to the Internet. The dataset consists of three protocol specific flooding attack traffic, namely, Ping ICMP flood, TCP SYN flood, and HTTP requests. In our experiment, we consider only the header information and remove the payload from all packets.

The DARPA 2000 dataset is generated using a scripted attack to break into a variety of hosts around the Inter-

[§] www.caida.org/data.

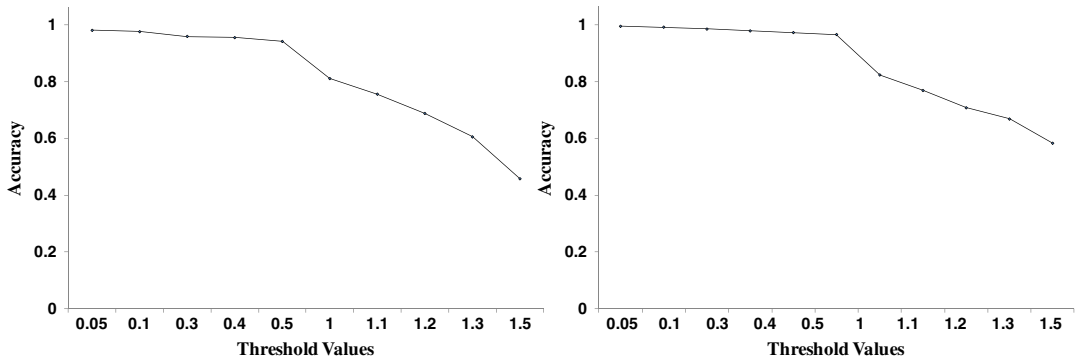
[¶] www.ll.mit.edu/ideval/data.

DOI: 10.1002/sec



(a) Accuracy on CAIDA dataset (b) Accuracy on DARPA dataset

Figure 4. Performance analysis without normalized datasets.



(a) Accuracy on normalized CAIDA dataset (b) Accuracy on normalized DARPA dataset

Figure 5. Performance analysis with normalizing datasets.

net, install the components necessary to run a Distributed Denial of Service attack, and then launch a DDoS attack at a US government site. As a part of the attack, the adversary uses the Solaris sadmind exploit, a well-known Remote-To-Root attack to successfully gain root access to three Solaris hosts at Eyrie Air Force Base. These attacks succeed due to the relatively poor security model applied at the AFB, with many services, including the dangerous "sunrpc" service, proxied through the base's firewall from outside to inside. The attacker uses the Mstream DDoS tool, a somewhat unsophisticated DDoS tools. It does not make use of encryption and does not offer as wide a range of attack options as other tools, such as TribeFlood-Network or Trinoo. An Mstream "server", the software that actually generates and sends the DDoS attack packets, is installed on each of the three victim hosts, while an Mstream "master", the software that provides a user interface and controls the "servers" is installed on one of the victims.

5.1.1. Result analysis without normalizing the dataset.

The proposed DDoS attack detection method shows high detection accuracy on the CAIDA as well as the DARPA dataset. The method compares captured network traffic samples with the normal profile. If the deviation between the normal profile and the test profile is greater than a user-defined threshold, an attack alarm is generated. So detection accuracy of the proposed method depends on various threshold values. However, the normal profile stores a parameter called N_{range} that keeps the range of possible values for FFSc in normal samples. This N_{range} is used to compute the similarity between normal samples and captured samples using FFSc. The difference is divided by N_{range}. Hence, the threshold value α should be in the range of 0.1 to 1.

On the CAIDA dataset, the method gives 100% detection accuracy for any values of α between 1 and 1.3, included. However, detection accuracy degrades gradually when the value of α is less than 0.5 and greater than 1.3. Similarly, in case of the DARPA dataset, the method gives 100% detection accuracy as shown in Figure 4(b). The method gives high detection accuracy for any values of α between 0.1 to 2, included.

5.1.2. Result analysis with normalizing the dataset.

The performance of the proposed DDoS detection method has also been evaluated on normalized datasets. Just before applying the analysis process, traffic objects

Table III. Performance comparison on CAIDA dataset.

Methods	DR	FPR	FNR
Identifier/location separation [13]	94.87%	3.85%	1.28%
Greedy algorithm [14]	93.20	12.1%	NA
Wavelet analysis using semi-supervise learning [15]	97.95%	1.75%	2.34%
Traffic flow [12]	95%	NA	NA
Cluster analysis [16]	99.77%	0.46%	0.31%
Proposed method	100%	0%	0%

DR, detection rate; FPR, false positive rate; FNR, false negative rate.

are normalized using z-score normalization. The proposed method gives high classification accuracy on both datasets after normalizing the data. As shown in Figure 5(a), the method yields 98% detection accuracy on the CAIDA dataset when the threshold value is 0.05 and the accuracy gradually decreases as the threshold value increases. If the threshold value is set to 1, the detection accuracy is reduced to 81.1%. Similar on the DARPA dataset, the method gives 99.55% detection accuracy for the threshold value 0.05. As shown in Figure 5(b), the performance of the proposed method decreases to 96.6% when the threshold is set to 1. We observe that the threshold range should be 0.05 to 0.8 (less than 1) to get high detection accuracy on both datasets.

5.2. Classification accuracy for low-rate and high-rate attacks

The difference between high-rate and low-rate attack traffic in terms of these four parameters is shown in Figure 3.

The proposed method gives high classification accuracy on high-rate and low-rate attack detection. The method classifies low-rate and high-rate attack based on attack intensity of the network traffic windows. If the attack intensity is greater than 0, the traffic window is marked as high-rate attack and otherwise the window is marked as low-rate attack. Low-rate and high-rate attack classification accuracy on the CAIDA dataset is 97.53% with 0.0087% false positive rate. Similarly on the DARPA dataset, the method gives 98.6% classification accuracy with 0.12% false positive rate.

5.3. Performance comparison of the proposed method with some existing methods

The proposed DDoS attack detection method was compared with five other competing methods such as Traffic flow [12], Identifier/location separation [13], Greedy algorithm [14], Wavelet analysis using semi-supervise learning [15] and Cluster analysis [16] in terms of detection rate, false positive rate, and false negative rate. The results obtained for CAIDA dataset are shown in Table III. It can be observed from Table III that the proposed method outperforms all other methods in terms of all three parameters. Although cluster analysis [16] was found superior among the other competing methods, the proposed method outperforms it with 100% detection rate. However, to achieve best possible performance, appropriate thresholding of these methods is highly essential. In case of our method, the best possible range of values for θ is (0.5–2.0) for non-normalized and (0.05–0.5) for normalized CAIDA and DARPA datasets, which provides the maximum accuracy.

6. CONCLUSION

An effective DDoS attack detection method has been reported, which uses a new statistical measure called FFSc. The method comprises two phases, nanmely, (i) classification of attack and normal traffic and (ii) classification of low-rate and high-rate traffic. It computes a similarity value using FFSc for each sample of network traffic and if the score is greater than a threshold, attack alarm is generated. The method computes attack intensity of a sample to detect the attack type either as low-rate or high-rate. The method was evaluated on two network datasets, and from the experimental results, it has been established that our method is superior in terms of detection rate, false positive rate, and false negative rate while comparing with its five other competing methods.

REFERENCES

1. Hoque N, Bhuyan MH, Baishya RC, Bhattacharyya D, Kalita JK. Network attacks: taxonomy, tools and systems. *Journal of Network and Computer Applications* 2014; **40**: 307–324.
2. Hoque N, Bhattacharyya DK, Kalita JK. Botnet in ddos attacks: trends and challenges. *Communications Surveys & Tutorials, IEEE*; **17**(4): 2242–2270.
3. Bhattacharyya DK, Kalita JK. *Network Anomaly Detection: A Machine Learning Perspective*. CRC Press: Taylor & Francis Group, Boca Raton, 2013.
4. Ahmed HA, Mahanta P, Bhattacharyya DK, Kalita JK. Shifting-and-scaling correlation based biclustering algorithm. *IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB)* 2014; **11**(6): 1239–1252.
5. Feinstein L, Schnackenberg D, Balupari R, Kindred D. Statistical approaches to DDoS attack detection and

response. *Proceedings of DARPA Information Survivability Conference and Exposition*, IEEE, Washington, DC, USA, 2003; 303–314.
6. Jin S, Yeung DS. A covariance analysis model for DDoS attack detection. *2004 IEEE International Conference on Communications*, IEEE, Paris, France, 2004; 1882–1886.
7. Peng T, Leckie C, Ramamohanarao K. Proactively detecting distributed denial of service attacks using source IP address monitoring. *2004*, Springer, Third International IFIP-TC6 Networking Conference, Athens, Greece, 2004; 771–782.
8. Xiang Y, Li K, Zhou W. Low-rate DDoS attacks detection and traceback by using new information metrics. *IEEE Transactions on Information Forensics and Security* 2011; **6**(2): 426–437.
9. Tan Z, Jamdagni A, He X, Nanda P, Liu RP. A system for denial-of-service attack detection based on multivariate correlation analysis. *IEEE Transactions on Parallel and Distributed Systems* 2014; **25** (2): 447–456.
10. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review* 2004; **34**(2): 39–53.
11. Hick P, Aben E, Claffy K, Polterock J. *The CAIDA DDoS attack 2007 dataset*, 2007.
12. Liu H, Sun Y, Valgenti VC, Kim MS. Trustguard: a flow-level reputation-based DDoS defense system. *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, IEEE, Las Vegas, Neveda USA, 2011; 287–291.
13. Luo H, Lin Y, Zhang H, Zukerman M. Preventing DDoS attacks by identifier/locator separation. *IEEE Network* 2013; **27**(6): 60–65.
14. Andrysiak T, Saganowski Ł, Choraś M. DDoS attacks detection by means of greedy algorithms. *Image Processing and Communications Challenges 4*, Springer, Bydgoszcz, Poland, 2013; 303–310.
15. Srihari V, Anitha R. DDoS detection system using wavelet features and semi-supervised learning, Springer Second International Symposium on Security in Computing and Communications (SSCC), Delhi, India, 2014; 291–303.
16. Bhaya W, Manaa ME. A proactive DDoS attack detection approach using data mining cluster analysis. *Journal of Next Generation Information Technology* 2014; **5**(4): 21–36.