Hindawi
Security and Communication Networks
Volume 2017, Article ID 3691629, 14 pages
https://doi.org/10.1155/2017/3691629

WILEY | Hindawi

Research Article

Low-Rate DDoS Attack Detection Using Expectation of Packet Size

Lu Zhou, Mingchao Liao, Cao Yuan, and Haoyu Zhang

School of Mathematics and Computer Science, Wuhan Polytechnic University, Wuhan 430023, China

Correspondence should be addressed to Mingchao Liao; lmingchao@whpu.edu.cn

Received 7 May 2017; Revised 6 July 2017; Accepted 31 July 2017; Published 11 October 2017

Academic Editor: Huaizhi Li

Low-rate Distributed Denial-of-Service (low-rate DDoS) attacks are a new challenge to cyberspace, as the attackers send a large amount of attack packets similar to normal traffic, to throttle legitimate flows. In this paper, we propose a measurement—expectation of packet size—that is based on the distribution difference of the packet size to distinguish two typical low-rate DDoS attacks, the constant attack and the pulsing attack, from legitimate traffic. The experimental results, obtained using a series of real datasets with different times and different tolerance factors, are presented to demonstrate the effectiveness of the proposed measurement. In addition, extensive experiments are performed to show that the proposed measurement can detect the low-rate DDoS attacks not only in the short and long terms but also for low packet rates and high packet rates. Furthermore, the false-negative rates and the adjudication distance can be adjusted based on the detection sensitivity requirements.

1. Introduction

Distributed Denial-of-Service (DDoS) attacks are a great threat on the Internet. Traditional DDoS attacks exhaust the bandwidth, CPU power, or memory of the victim host by flooding an overwhelming number of packets from thousands of compromised computers (zombies) to deny legitimate flows. The frequency of such attacks has been rapidly growing since the year 2000, and a recent survey found that the largest DDoS attack achieved 453.8 Gbps in December 2014 [1]. As they heavily rely on the high-rate transmission of packets, these attacks present obvious statistical anomalies and can be detected [2–7]. However, the problem of DDoS detection is made more severe by the evolution of the low-rate DDoS attacks. Low-rate DDoS attacks are quite different from the traditional DDoS attacks, as their traffic is similar to legitimate traffic. A low-rate DDoS attacker exploits the vulnerability of TCP's congestion-control mechanism by periodically sending burst attack packets over short periods of time repeatedly (pulsing attack) or continuously launching attack packets at a constant low-rate (constant attack). As these attacks reduce the average number of attack packets to avoid being detected by existing detection schemes, it is difficult to distinguish such attacks from legitimate traffic with a large measurable distance gap and a low false-negative rate.

The existing DDoS attack-detection metrics can be divided into two categories: signature-based metrics and anomaly-based metrics [8]. The signature-based metrics rely on the matching of special patterns to the tested traffic. In low-rate DDoS attack detection, for example, a typical signature used in the signature-based metric is the burst (pulse) period [9, 10]. The burst period is usually used by low-rate DDoS attackers to explore the homogeneity of the minimum retransmission timeout (RTO), and a widely applied value of the burst period is 1 second [10] in such detection metrics. However, a recent study demonstrated that this value is inaccurate, as it does not consider the network environment [11], for example, traffic congestion, especially when an attack is ongoing. Therefore, in general, the common defect of signature-based metrics is vulnerability when the signature pattern is unknown. On the other hand, the anomaly-based detection methods depend on identifying obvious statistical anomalies by comparison against the legitimate traffic. Entropy, for instance, is commonly used in anomaly-based metrics. The entropy variation between

normal traffic and tested traffic may indicate that the entropy value of the tested traffic is anomalous and, therefore, a low-rate DDoS attack is occurring [8]. However, the limitation is that the value of the entropy gap is quite small, which could raise a lot of false alarms. In this paper, we propose an expectation of packet size (EPS) measurement to distinguish attack traffic from legitimate traffic. The proposed method is independent of the attack pattern; therefore, it can avoid the inherent shortcomings of the signature-based metric. Moreover, our approach can achieve a large distance gap between the attack traffics and the legitimate traffics, which could further contribute to a low false-positive rate.

Our contributions are summarized as follows:

(i) We analyze the distribution difference of the packet size between the low-rate DDoS attacks and the legitimate traffic.

(ii) We propose an EPS-based approach to measure the distribution difference of the packet size, and the proposed measurement can distinguish the low-rate DDoS attacks from the legitimate traffic.

(iii) We conduct intensive simulations using real datasets to demonstrate that the distance gap of the proposed measurement is large but the false-negative rate is small.

(iv) The proposed method is independent of network topology, arrival patterns, and pulse patterns of attack packets.

The rest of the paper is organized as follows. Section 2 describes and analyses our expectation of packet size model. Contrast experiments are conducted in Section 3. Intensive simulations using real datasets are presented in Section 4. Section 5 reviews previous work, and we summarize the paper and discuss future work in Section 6.

2. Detection Algorithm

In this section, we propose and analyze our method. As the Internet was designed for openness and best-effort transmission, legitimate packets, as well as attack packets sent by malicious users, can be easily forwarded by current network-transmission mechanisms. Particularly in the case of low-rate DDoS attacks, attack traffics exhibit specific anomaly characteristics, such as the number of flows and packets that present differences in distributions or statistics compared with those of legitimate traffics. For example, an anomaly characteristic of low-rate DDoS attacks is that every single packet forwarded in the network is legitimate since the packet's head information fulfills all legal requirements of the network-transmission protocols; however, the intentional aggregation of these packets at victim hosts by attackers exhibits abnormal statistical deviations [12]. In addition, as the low-rate DDoS packets are purposely created by prebuilt programs, the features of these packets are highly similar [13, 14]. These features must affect the natural patterns in the normal network, which are usually random due to the complexity and dynamics of the real network [8]. In this study, we focus on the distribution difference of the packet size between the attack packets and the legitimate packets and find that the distribution difference of the packet size can be measured. Furthermore, this measured difference can be used to distinguish attack traffic from legitimate traffic. That is, for the purpose of best-effort transmission of attack packets, attackers usually generate small packets or even empty packets to reduce the resources required while, in contrast, although the packets of communication protocols are also small, packets filled with user data, which are normally large, make up a considerable percentage of the legitimate traffic. Therefore, this distribution difference between attack traffic and normal traffic can be measured by our expectation of packet size.

We classify packets into network flows and cluster network flows, which share the same destination address as one of the network flows. Let $X(t)$ take values $x_1, x_2, \ldots, x_n$ in different network flows at time t. For a given time interval Δt, we denote by $c_i(\Delta t)$ the number of packets of the ith network flow $x_i(\Delta t)$, by l_{ik} the packet size of the kth packet, and by $l_{i\max}$ the maximum packet size of the ith network flow. According to our knowledge, a network flow may have packets of many different sizes due to different types and contents. Therefore, we classify the network flows by packet size. For each flow, the network flow $x_i(\Delta t)$ is defined as

$$x_i(\Delta t) = \{x_i(l_{i1}), x_i(l_{i2}), \ldots, x_i(l_{ik}), \ldots, x_i(l_{i\max})\}. \quad (1)$$

We should note that the packet size is limited by the network protocol. The most widely used network protocol is Digital Equipment Corporation, Intel, Xerox (DIX) Ethernet V2. According to DIX Ethernet V2, the minimum packet size is 64 bytes, and the maximum packet size is 1518 bytes, which is composed of the Maximum Transmission Unit (MTU) (1500 bytes) [15] and the Ethernet head (18 bytes). However, Frame Check Sequence (FCS, 4 bytes) in the Ethernet head will be dropped after the packet is checked. Therefore, the packet size received on the receiver side satisfies $60 \le l_{ik} \le 1514$. In the rest of the paper, for simplicity, we set the minimum packet size to 60 bytes and the maximum to 1514 bytes.

As a part of packet header, the packet size is an independent attribute in a packet. In theory, it is independent of packet types, such as TCP and UDP, and packet cluster methods, for example, source or destination-based traffic flow. Therefore, for each packet, regardless of the packet type and the packet cluster method, we directly read the packet size from the packet header into a set of packet size $L(\Delta t)$. The packet size set $L(\Delta t)$ in the interval Δt is defined as

$$L(\Delta t) = \begin{pmatrix} l_{11} & l_{12} & \cdots & l_{1\max} \\ l_{21} & l_{22} & \cdots & l_{2\max} \\ \cdots & \cdots & l_{ik} & \cdots \\ l_{n1} & l_{n2} & \cdots & l_{n\max} \end{pmatrix}. \quad (2)$$

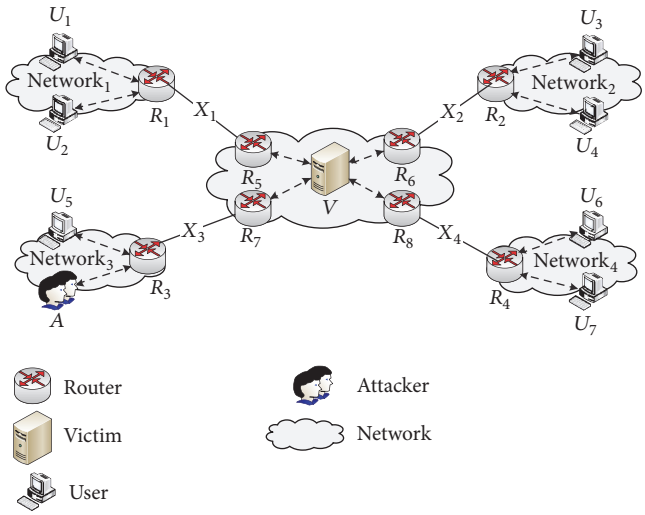

Figure 1: A simple scenario of low-rate DDoS attacks on a victim.

The mean of packet size of network flow x_i is

$$\overline{l}_i = \frac{1}{c_i} \sum_{k=1}^{c_i} l_{ik}, \tag{3}$$

where $60 \le \overline{l}_i \le 1514$.

Here, the probability of occurrence of x_i, that is, $p(X) = \{p(x_1), p(x_2), \ldots, p(x_n)\}$, is calculated as

$$p(x_i) = \frac{c_i}{\sum_{i=1}^{n} c_i}. \tag{4}$$

Following this definition, we know that $p(x_i) \ge 0$ and $\sum_{i=1}^{n} p(x_i) = 1$.

The expectation of the packet size of the network flow X is

$$E(X) = \sum_{i=1}^{n} p(x_i)\, \overline{l}_i. \tag{5}$$

We now discuss the symmetry property of the EPS.

Assertion. A simple topological graph of low-rate DDoS attacks on a victim is shown in Figure 1. Suppose that $X = \{x_1, x_2, x_3, x_4\}$ is the ordered flows in the sample time Δt and $T = \{t_1, t_2, t_3, t_4\}$ is the set of end times of the last packet received in the sample time for the ordered flows X ($T \in \Delta t$). Then, $t_1 < t_2 < t_3 < t_4$. Let the probability of each flow be $P = \{p_1, p_2, p_3, p_4\}$, and let $\overline{L} = \{\overline{l}_1, \overline{l}_2, \overline{l}_3, \overline{l}_4\}$ take values of the mean packet size of X. Without loss of generality, suppose that attackers hide in network 3. We have the following symmetry property of the EPS:

$$E\{x_1, x_2, x_3, x_4\} = E\{x_3, x_1, x_2, x_4\}. \tag{6}$$

The symmetry property implies that the EPS is independent of the packet arrival patterns and pulse patterns because the EPS value is not related to the packet arrival time and end time in the sample time. Therefore, the EPS can avoid the shortcoming of inaccuracy caused by network congestion [16]. In addition, since the EPS is independent of the order of the flows, the value of the EPS remains unchanged if the attacker changes his position, for example, from network 3 to network 2 in Figure 1. That is, the EPS is also independent of the topology of network flows, as the value of the EPS does not depend on which network the flows come from or the order of the flows. Moreover, the measurement could be used not only for real-time detection but also for nonreal-time dataset analysis after a dataset is captured. According to the above discussion, we can use both offline and online datasets to test our method.

As we mentioned above, the distribution of the packet size is expected to change when a low-rate DDoS attack is ongoing. Specifically, the EPS of attack traffic is expected to be considerably smaller than that of normal traffic and to vary within a narrow limit. Motivated by this difference, we propose the following inequality to distinguish between low-rate DDoS attack traffic and normal traffic:

$$E(A) + \alpha d \le E(N), \tag{7}$$

where $E(A)$ and $E(N)$ are the EPSs of attack traffic and normal traffic, respectively. $\alpha \in R$, where R is the set of real numbers. The parameter α is the tolerance factor, and d is the variance of the attack traffic in terms of the EPS.

$$d = \sqrt{\frac{\sum_{i=1}^{n} \left(E(A) - \overline{l}_i\right)^2}{n}}. \tag{8}$$

We denote $E(A) + \alpha d$ by EPSV for short and $E(N)$ is the EPSV of the normal traffic when $\alpha = 0$.

For the aim of describing the distance gap between normal traffic and attack traffic directly, we let $D(\alpha, \Delta t)$ represent the distance in the interval t.

$$D(\alpha, \Delta t) = E(N) - (E(A) + \alpha d). \tag{9}$$

Suppose that we have obtained and stored the normal EPS, $E(N)$, in advance without attack and sample M network flows in the time interval t, $x_1, x_2, \ldots, x_M$. Therefore, we can obtain the sampled EPS $E(S)$. Let I_M be the indicator for the relation between $E(N)$ and $E(S)$. I_M has only two possible values: 1 for low-rate DDoS attack and 0 otherwise. Then, we have

$$I_M = \begin{cases} 1, & D(\alpha, \Delta t) \ge 0, \\ 0, & D(\alpha, \Delta t) < 0. \end{cases} \tag{10}$$

According to the above discussion, we design the EPS algorithm as shown in Figure 2 and Algorithm 1 to detect a low-rate DDoS attack.

3. Experimental Results

In this section, we demonstrate the effectiveness of the EPS in detecting low-rate DDoS attacks. For the aim of determining

Input:
Sample time Δt;
Tolerance factor α;
Obtained $E(N)$.
Output:
Low-rate DDoS attack indicator I_M.
(1) According to sample time Δt, sample packets;
(2) Cluster packets by network flow;
(3) Determine the statistics of the packet size and calculate the mean packet size of each flow;
(4) Calculate the probabilities of network flows;
(5) Calculate the expectation of packet size $E(S)$ and variance d;
(6) According to formula (10), set I_M;
(7) **return** I_M

Algorithm 1: Low-rate DDoS attack detection using the expectation of packet size.

the distance gap of the EPS between low-rate DDoS attack traffic and legitimate traffic, we should analyze and calculate the statistical difference in packet size between them. In this detection, investigating the distribution differences and the distance gap of the packet size is the main issue. Therefore, we first analyze the packet-size distribution of the legitimate traffic and present the scope of the EPS. Then, for comparison, the distributions and the variances of two typical low-rate DDoS attacks are presented together with the value of the EPS. Finally, we summarize the distribution differences in the form of the EPS and test the effectiveness of the proposed measurement.

3.1. The Packet Size of Legitimate Traffic. The packet size of legitimate traffic has huge fluctuations and varies with the protocols and user data in the real daily Internet scenario. Legitimate traffic, which includes communication-protocol packets and user-data packets, has a predictable packet size in normal situations. Specifically, for the purpose of effectiveness, most communication-protocol packets have predefined specified packet sizes in the network. For example, an ACK packet in the three-way handshake, which is the process of TCP connection establishment, is always of size 60 bytes. Particularly, we should note that the packet sizes of SYN packets are approximately 62 bytes because these packets are the main packets in the SYN Flooding DDoS attack. In conclusion, normally, the packet sizes of communication-protocol packets in legitimate traffic are small in the daily Internet. The packet sizes of user-data packets, on the other hand, are large. For the aim of great efficiency, the sizes of user-data packets can easily reach the MTU. The MTU is the maximum packet size that the data-link layer can transmit and is usually 1500 bytes in Ethernet v2. A typical frequently used user-data packet, for example, the Hypertext Transfer Protocol (HTTP) packet, can easily reach the MTU in the data unit, and the whole packet size can reach 1514 bytes, including the packet head. In low-rate DDoS attack detection, however, the packet size of a single legitimate packet, regardless of whether the communication-protocol packet or user-data packet is included, is very difficult to detect as abnormal, as each packet is a legitimate packet, but these purposefully aggregated packets are a DDoS attack. Therefore, it is necessary to use several real legitimate datasets from different trace times to investigate the distributions and the expectations of packet size.

The first legitimate dataset we used is a daily traffic trace taken from 12:30 to 12:45 on 2007-01-10 UTC [17], shown in Figure 3. This legitimate dataset was collected from a 100-Megabit Ethernet link that connects the Widely Integrated Distributed Environment (WIDE) [18] backbone network in Tokyo, Japan and, more importantly, is a part of the "A Day in the Life of the Internet" (DITL) project [19]. The DITL project, which consists of large-scale simultaneous collections from critical components of the global Internet infrastructure, is considered as a prototype for Internet events of the day. The packets in the dataset contain full head information, including packet size; therefore, the dataset is suitable for investigating the EPS of legitimate traffic. In the rest of this paper, all legitimate-traffic data come from the DITL project.

Figure 4 illustrates the probability distribution of the packet size of the first legitimate dataset, and it directly determines the EPS. Obviously, there are two probability peaks in the figure: the first peak occurred at around 60 bytes and the second at 1514 bytes. We further investigate these two peaks and find that the probability of the packet size peaked at around 60 bytes because communication-protocol packets, such as ACK packets and ICMP packets, make up a considerable percentage of the legitimate traffic and most of these packets are approximately 60 bytes in size. The second probability peak, on the other hand, is at 1514 bytes since all packets in the second probability peak are user-data packets (most of them are HTTP packets) and these user-data packets are the other main packets in the legitimate traffic. For a DDoS detection based on packet size, these two probability peaks are the main influence factors of the EPS in the legitimate dataset. We calculate the EPS of the first legitimate dataset using formula (5), and the result is 726.1894 bytes.

However, the use of only one dataset to investigate the EPS of a legitimate dataset is insufficient, as the EPS of a legitimate dataset may fluctuate at different times. Therefore,

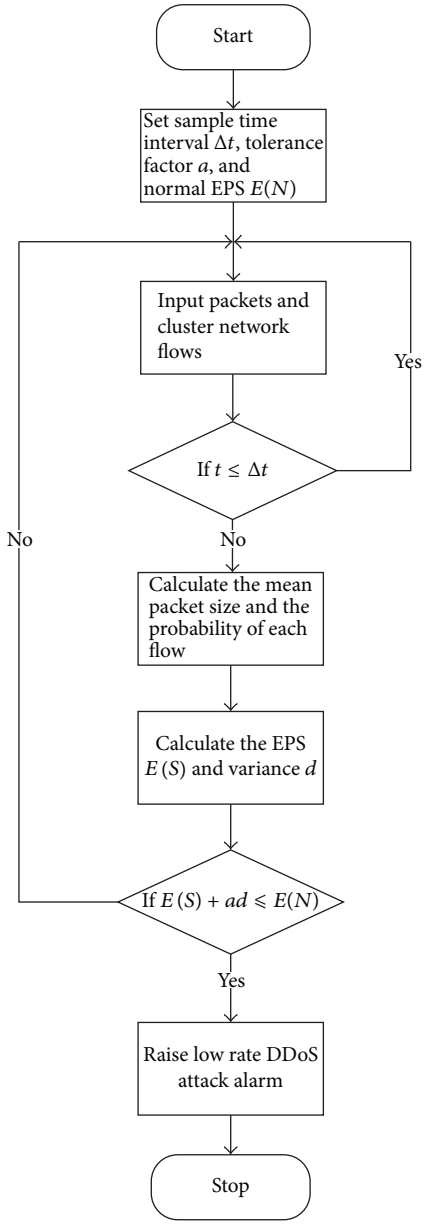

Figure 2: Detection flowchart.

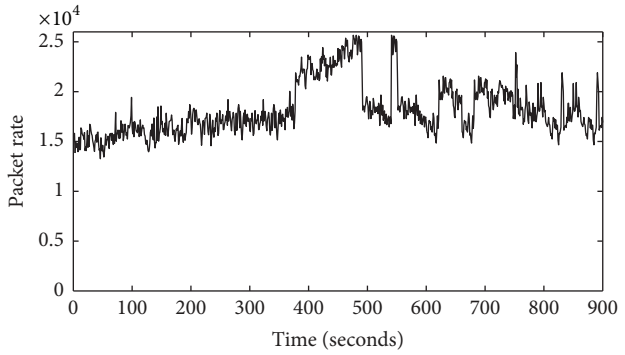

Figure 3: The legitimate-traffic scenario sampled from 12:30 to 12:45 in 2007-01-10.

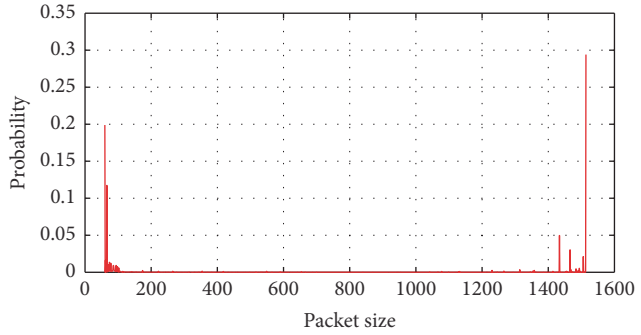

Figure 4: The probability distribution of the legitimate traffic sampled from 12:30 to 12:45 in 2007-01-10.

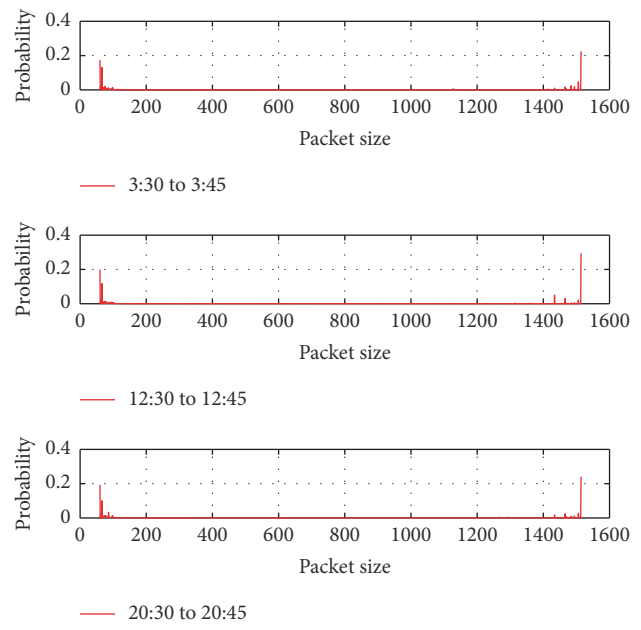

Figure 5: The comparison of the probability distributions from 2007-01-10.

it is essential to investigate the EPS in different time periods throughout the day and even in different years.

First, we investigate the fluctuation of the EPS for the legitimate datasets in different time periods in a day. The EPS of legitimate traffic may fluctuate at different times in a day due to the dynamic nature of the Internet traffic. For a fair comparison, two more datasets with the same duration from 2007-01-10 are chosen: one dataset is from 3:30 to 3:45 UTC, and the other is from 20:30 to 20:45 UTC. The probability distributions of the packet size on this day are shown in Figure 5. Figure 5 illustrates that the probability distributions of these three datasets are quite similar to one another in terms of the two main peaks. On the other hand, we calculate the EPSs of these datasets using formula (5), and the results are listed in Table 1. From Table 1, we can see that it is true that the EPS of legitimate datasets fluctuate during the day; however, the lower bound for the day still remains at around 650 bytes. Therefore, we can conclude that the EPSs of the

Table 1: The EPSs of the legitimate-traffics samples at different times on 2007-01-10.

Start time	End time	EPS (bytes)
3:30	3:45	658.2429
12:30	12:45	726.1894
20:30	20:45	649.5250

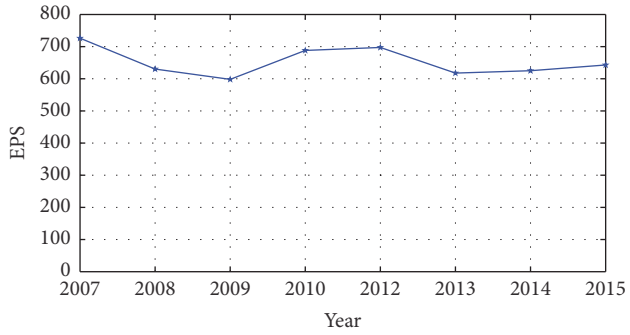

Figure 6: The EPSs of the legitimate-traffic samples from the eight different years.

legitimate datasets fluctuate over the day but still remain large.

In addition, we investigate the EPSs of legitimate datasets, which vary with the years. With the increasing development of applications for servers and increasing demands from clients, the EPSs of legitimate traffic in different years may fluctuate to some extent. To investigate the fluctuation, eight legitimate datasets with the same duration from different years are chosen, and the details are shown in Table 2. We calculate the expectation of packet size for these eight datasets, and the results are shown in Figure 6. These examples show that although the numbers of legitimate packets in these years are growing in general, the EPS still remains at a high level.

In conclusion, the above experiments have demonstrated that the EPS of legitimate traffic maintains a large value, not only at different times in a day but also in different years. That is, the first factor, $E(N)$ in formula (7), maintains at a large value.

3.2. The Packet Size of Low-Rate DDoS Attacks. The low-rate DDoS attacks have quite different distributions of packet size. Generally, the key feature of DDoS attacks is the resource battle between the victims' servers and attackers' botnets. A successful DDoS attack occurs when the packets of the attacker are more than the victim can handle. Therefore, with the aim of sending as many malicious packets as possible, attackers generate few types of packets, such as SYN packets and ICMP packets, and more importantly, these packets are similar in size because of the low cost of computing resources. In this section, two typical low-rate DDoS attacks are chosen to investigate the expectations and variances of the packet size in attack traffic.

The constant attack, which generates attack packets at a constant low rate, is the first low-rate DDoS attack that we examined. The dataset we chose comes from the Center of

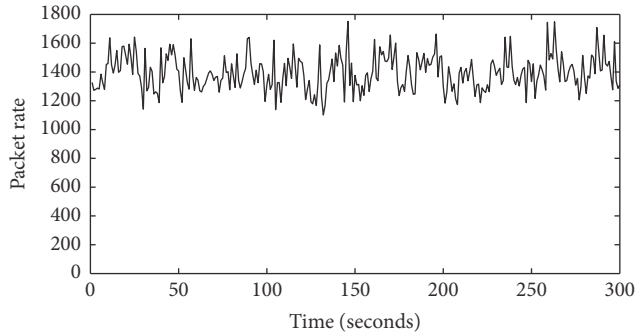

Figure 7: The constant attack traffic scenario.

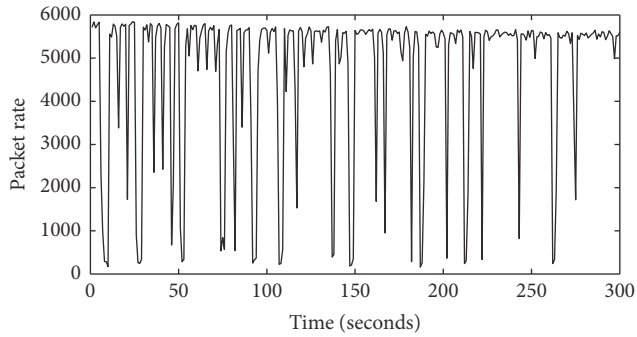

Figure 8: The pulsing attack traffic scenario.

Applied Internet Data Analysis (CAIDA) [20], and the 5-minute sample of data traffic that occurred on 2007-08-22 at 07:00 UTC is shown in Figure 7. The average packet rate is approximately 1400, and the variance rate is 200; thus, based on [8], this is a low-rate DDoS attack dataset. On the other hand, the second type of low-rate DDoS attack is a pulsing attack, in which attack packets are sent periodically to victims. The dataset, which also comes from CAIDA and is traced from 14:34:36 to 14:39:36, is another 5-minute dataset from 2007-08-04 UTC, and the attack scenario is shown in Figure 8. Both of these datasets are low-rate attacks since the rates of attack packets and the attack patterns exhibit the features of low-rate DDoS attacks [10].

The probability distributions of the packet size of the constant attack and the pulsing attack are quite different compared with that of legitimate traffic. Figure 9 shows the probability distributions of the packet size of these two low-rate DDoS attacks. In Figure 9, the probability of the constant attack is decreasing at an exponential rate. It begins with the maximum value, 0.63, at a packet size of 60 bytes and decreases to nearly 0 at 200 bytes. As for the pulsing attack, the probability of the packet size is more concentrated, even compared with the constant attack, let alone the legitimate traffic. This clearly shows that most of the pulsing attack packets are concentrated in a very limited range and that no packet is larger than 100 bytes. Further investigation shows that these packets are ICMP attack packets and that, more importantly, 93.91% of the packets are 88 bytes in size. Therefore, we can see that the distributions of both of these attacks are concentrated at small packet sizes.

Table 2: The details of datasets from eight different years.

Date	Start time	End time	Packets	Average packet rate
2007-01-10	12:30	12:45	16,199,453	17999
2008-03-18	12:30	12:45	14,738,786	16376
2009-03-30	12:30	12:45	16,759,289	18621
2010-04-13	12:30	12:45	34,009,901	37788
2012-03-30	12:30	12:45	25,248,668	28054
2013-06-27	12:30	12:45	74,274,342	82527
2014-12-10	12:30	12:45	131,471,390	146079
2015-12-02	12:30	12:45	117,233,904	130259

Table 3: The comparison of the EPS and variance between the legitimate traffic and the attack traffic samples (units: bytes).

	Pulsing attack	Constant attack	Legitimate traffic
EPS	87.2663	76.4786	756.1894
Variance	3.1434	76.0008	690.4353

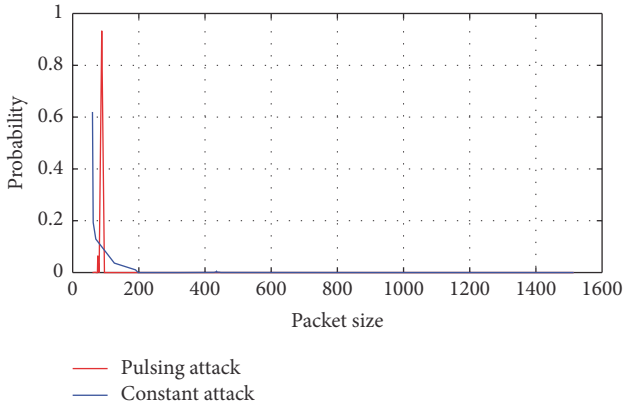

Figure 9: The probability distributions of the constant attack and pulsing attack.

The concentrated distributions of the packet size of the low-rate DDoS attacks contribute to large EPS gap of between the attack traffic and the legitimate traffic. Figure 10 shows the cumulative probability distributions of the packet size for the two low-rate DDoS attacks and the legitimate traffic from 2007-01-10 UTC 12:30. It clearly shows that the packet sizes of these two attacks are concentrated at small values, while the packet sizes of legitimate traffic are concentrated at both small and large values. Therefore, this distribution difference between attack traffic and legitimate traffic results in a large EPS gap. We calculate the variances and the expectations of packet size for the attack datasets and the legitimate dataset (shown in Table 3). Table 3 shows that both the expectations and the variances of the constant attack and the pulsing attack are small; on the contrary, those of the legitimate dataset are large. This indicates that the packet sizes of the attacks are small and steady compared with the legitimate traffic.

To sum up, the packet size of constant attack and pulsing attack is small and concentrated. This means that, in formula (7), the value of the second parameter, $E(A)$, which is the

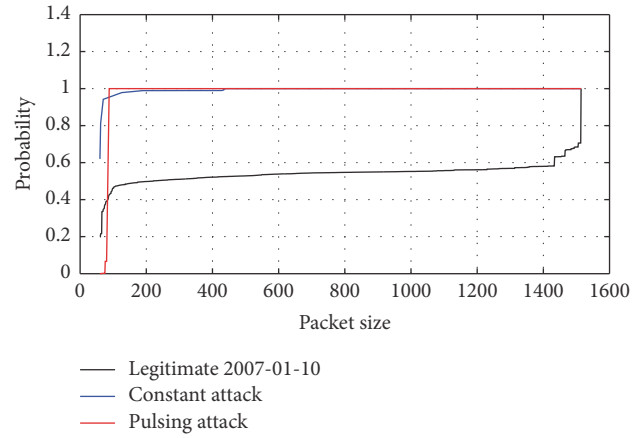

Figure 10: The comparison of the cumulative probabilities of the legitimate traffic and the two attack traffic samples.

EPS of the low-rate DDoS attack, is smaller than the EPS of legitimate traffic, $E(N)$.

3.3. Detection Mechanism. Given the discrepancies of the probability distributions and the EPS distance between the low-rate DDoS attacks and the legitimate traffic, we present our packet-size-based method to distinguish the low-rate DDoS attacks from the legitimate traffic.

Although it has been demonstrated that the EPS of the legitimate traffic is greater than that of the low-rate DDoS attacks, the EPS in a network may change dynamically and the false-negative rate may be high due to the stochastic nature of network traffic. Consequently, the variance of the packet size of an attack, which is used to measure the degree of deviation of the attack traffic from its expectation, is chosen as the third factor in the proposed approach. It has been observed that the variances of the packet size of low-rate DDoS attacks are small, and therefore, the packet sizes of most attack packets are close to their expectations. However, only using the parameter $E(A) + d$, which represents the statistical range of the packet size of the low-rate DDoS attacks, to detect the attacks may be too narrow of an approach due to the dynamic characteristic of packet size (which ranges from 60 bytes to 1514 bytes). Therefore, another parameter, the tolerance factor α, is set to investigate the range of EPSV in a statistical manner.

Table 4: The values of EPSV and the ratios of EPSV along with α.

α	EPSV (bytes)		R_{EPSV}	
	Pulsing attack	Constant attack	Pulsing attack	Constant attack
0	87.26	76.47	6.06%	91.54%
1	90.40	152.47	99.98%	95.61%
2	93.55	228.48	99.98%	98%
3	96.69	304.48	99.99%	98%
4	99.83	380.48	99.99%	98%
5	102.98	456.48	99.99%	99.54%
6	106.12	532.48	99.99%	99.55%
7	109.27	608.48	99.99%	99.55%
8	112.41	684.48	99.99%	99.55%
9	115.55	760.48	99.99%	99.55%
10	118.70	836.48	99.99%	99.55%

The tolerance factor α is used to adjust the distance gap according to the detection-accuracy demands and dynamic network situations. Combined with the variance d of the tested traffic, the parameter $\alpha * d$ represents the fluctuation degree of the packet size in the traffic. For a given test traffic sample, the greater α is, the greater the parameter $\alpha * d$ is, which makes EPSV, $E(S) + \alpha * d$, represent more tested packets. We use R_{EPSV} to denote the ratio of the low-rate DDoS attack packets represented by EPSV. Then, we have $R_{EPSV} = N_{EPSV}/N_A$, where N_{EPSV} is the number of attack packets represented by EPSV and N_A is the total number of attack packets. Table 4 shows that, for both the pulsing attack and the constant attack datasets, the values of R_{EPSV} are increasing with the tolerance factor α. In addition, R_{EPSV} of the traffic can achieve stable values while $\alpha > 2$ for both types of attack. More importantly, while R_{EPSV} of those attacks achieves stable values, the values are very close to 1. For example, in this experiment, the EPSV can represent 99.99% and 99.55% of the pulsing attack packets and the constant attack packets, respectively, while the order $\alpha = 6$.

Now, we discuss the relationship between the EPS of the legitimate traffic, $E(N)$, and the range of the packet size of the attack traffic, EPSV, along with the order α, which directly determines the distance gap between the legitimate traffic and the attack traffic. In this experiment, we compare the values of the EPSV of the two low-rate DDoS attack traffic samples, which vary with the order α, and the EPSs of the eight real legitimate datasets in Table 2 (the results are shown in Figure 11). In Figure 11, we can see that, for the pulsing attack, all EPSs of these eight legitimate datasets are far beyond the EPSV of the pulsing attack, even when the order $\alpha = 10$. As a result, the proposed measurement will detect the low-rate DDoS attacks according to formula (10). On the other hand, although the EPSV of the constant attack is greater than the EPSs of the legitimate datasets when the order $\alpha > 7$, the proposed measurement can still detect 99.55% of the constant attack packets when the order $\alpha = 6$ according to Table 4. Therefore, we can detect the constant attack when $\alpha \leq 6$. It should be noted that an inappropriate choice of α might cause false-negative alarms since the EPSV increases progressively with α. We will further discuss the choice of α in Section 4.

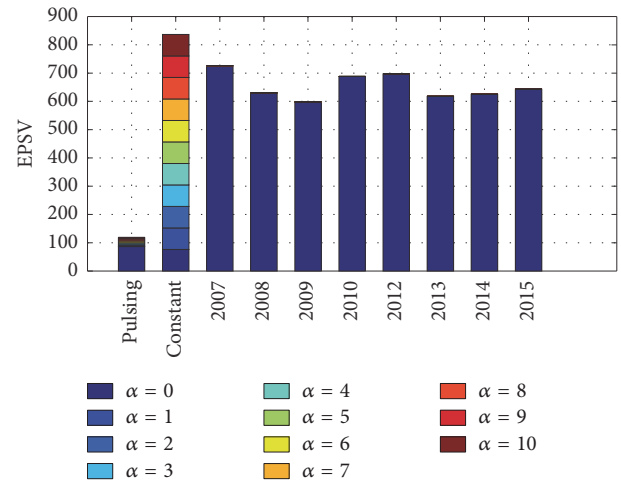

Figure 11: The comparison of the EPSs of the legitimate traffics in different years and the EPSVs of the attack traffic samples.

To sum up, we can see that the probability distributions of the packet size of the legitimate traffic and the low-rate DDoS attacks have great differences, and therefore, there is a distance gap between the legitimate traffic and the attack traffic based on the EPS. Specifically, the EPS value of legitimate traffic is independent of time, and more importantly, it stays at a high level. On the other hand, the EPS values of both typical low-rate DDoS attacks are quite small, and moreover, they fluctuate within very limited ranges. In conclusion, the proposed measurement is stable in measuring the EPS of the legitimate traffic and the EPSVs of the attack traffic, and the distance gap between the EPS and the EPSV can be used to distinguish the real attack datasets from the real legitimate datasets.

4. Performance Evaluations

4.1. Effectiveness of the Proposed Measurement. With the aim of evaluating the performance of the proposed measurement, two practical factors in DDoS attack detection are considered

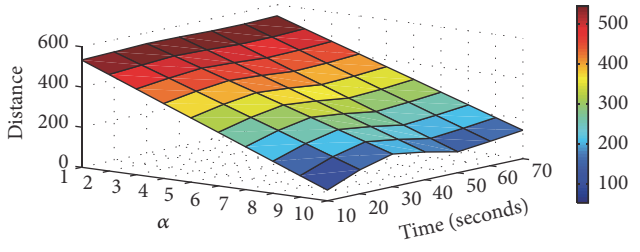

Figure 12: The distances between the EPSs of the legitimate traffic and the EPSVs of the constant attack traffic samples in short terms.

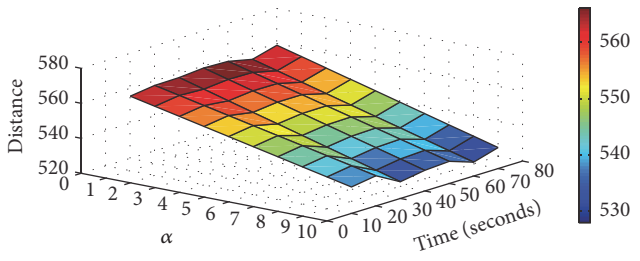

Figure 13: The distances between the EPSs of the legitimate traffic and the EPSVs of the pulsing attack traffic samples in short terms.

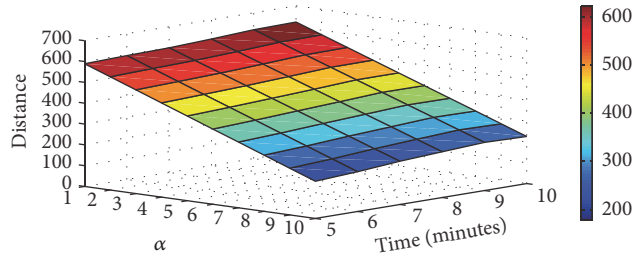

Figure 14: The distances between the EPSs of the legitimate traffic and the EPSVs of the constant attack traffic samples in long terms.

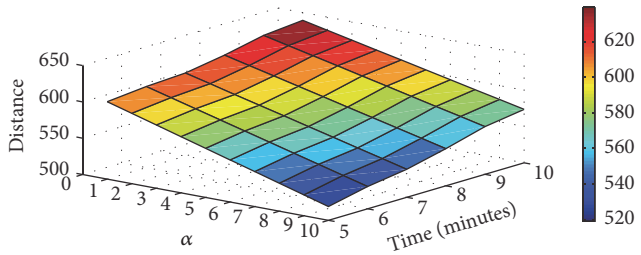

Figure 15: The distances between the EPSs of the legitimate traffic and the EPSVs of the pulsing attack traffic samples in long terms.

in this section to test the robustness and effectiveness of the proposed measurement: the duration of the attack and the rate at which the attack packets are sent.

The duration of the low-rate DDoS attack is an important factor in low-rate DDoS attack detection for two reasons. First, to avoid being detected, a normal DDoS attack usually would not last for a very long time; for example, 10 minutes is the normal duration of attack [14]. Consequently, as a basic function of a detection measurement, it is essential to detect quickly the attacks of short duration. Second, a low-rate DDoS attacker may keep sending attack packets for a long time because of the key feature of the attacks: the attack packets are sent at a low average rate. For these reasons, it is essential to test a low-rate DDoS detection measurement not only in the short term but also in the long term.

First, a series of short-term simulations with different orders of α are conducted for the performance estimation of short-term detection. For both the legitimate traffic and the attack traffic, we increase the duration of these traffic samples gradually to observe the distance gaps $D(\alpha, \Delta t)$ with different α. We slowly increase the simulation time from 10 seconds to 70 seconds, and the experimental results are shown in Figures 12 and 13, respectively. Obviously, two important points are illustrated by both of these figures. First, for a given time, for example, 10 seconds, although the distance gap $D(\alpha, \Delta t = 10)$ is decreasing as the order α increases, the distance gap $D(\alpha, \Delta t = 10)$ is still nonnegative due to the large distance between the legitimate traffic and the two low-rate DDoS attack traffic samples measured by the EPS. (We should note that the shortest duration of the simulation, $\Delta t = 10$ s, is a conservative choice. It is not the fastest detection time in our measurement. In this paper, the choice of $\Delta t = 10$ can be set as a preset sample time.) Second, keeping the order α unchanged, the distance gaps, for example, $D(\alpha = 6, \Delta t)$, fluctuate in a small limited range with the increase in duration; more importantly, all these distance gaps are greater than 0. To sum up, for both the legitimate traffic and the attacks traffic, the EPSs can achieve stable values within a short time, and moreover, these stable values are measured by the EPS directly and contribute to the huge distance gaps between the legitimate traffic and the attack traffic. Therefore, the proposed measurement can distinguish the low-rate DDoS attacks from the legitimate traffic within in a short time.

Second, simulations of long-term detection using the EPS are performed to demonstrate the effectiveness of our proposed measurement. As we mentioned above, generally, a DDoS attack does not last very long, and the average duration is 5–10 minutes. Thus, 6 datasets, each lasting from 5 minutes to 10 minutes, are randomly sampled from the legitimate traffic and the attack traffic to investigate the detection effectiveness in long-term attacks. The results are shown in Figures 14 and 15, and they indicate that, similar to the short-term detection, the proposed measurement can detect the low-rate DDoS attacks, as all the distance gaps are nonnegative for all orders of α over the long terms. Furthermore, we should note that the distance gaps of the long terms are more stable than those of the short terms, with better convergence of the distance gaps for the long-term datasets.

In addition to the duration of the attack, the attack-packet rate is another factor in evaluating the detection performance of our proposed measurement. The packet rate, which is the main difference between a high-rate DDoS attack and a low-rate DDoS attack, changes dynamically due to the stochastic nature of Internet traffic. Due to the similarity of the packet rates between low-rate attacks and legitimate traffic, detecting

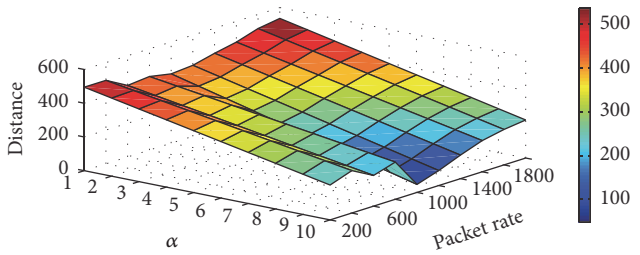

Figure 16: The distances between the EPSs of the legitimate traffic and the EPSVs of the constant attack traffic samples at low packet rates.

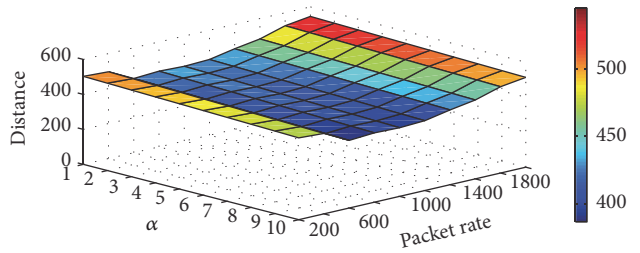

Figure 17: The distances between the EPSs of the legitimate traffic and the EPSVs of the pulsing attack traffic samples at low packet rates.

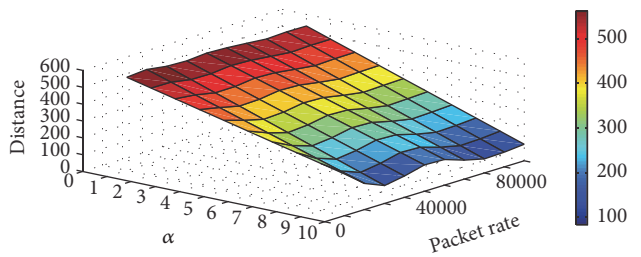

Figure 18: The distances between the EPSs of the legitimate traffic and the EPSVs of the constant attack traffic samples with high packet rates.

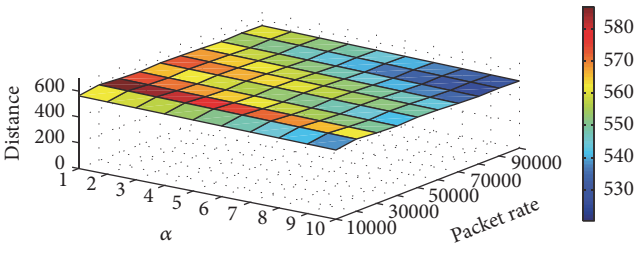

Figure 19: The distances between the EPSs of the legitimate traffic and the EPSVs of the pulsing attack traffic samples with high packet rates.

such attacks under the condition of the same packet rate, especially a low packet rate, is significant in low-rate DDoS attack detection. Meanwhile, combining Table 2 and Figures 7 and 8, we can see that the rate of the legitimate packets is larger than the rate of the attack packets and has continued to increase in recent years. Consequently, it is necessary to demonstrate the effectiveness of the detection measurement in scenarios with a high packet rate. Therefore, considering these situations together, a good detection mechanism should be able to detect abnormal deviations regardless of whether the packet rate is low or high.

The low packet rate, which is the key characteristic of the low-rate DDoS attacks for exploiting the vulnerabilities of congestion control, is taken into consideration when evaluating the performance of the proposed measurement. In this experiment, we increase the packet rate from 200 packets per second to 2000 packets per second gradually since it has been shown that the typical packet rate of low-rate DDoS attacks is approximately 1000 packets per second [8]. Figures 16 and 17 illustrate that, for both the constant attack and the pulsing attack, the proposed measurement is effective in the following two aspects: First, for a given packet rate, for example, 200 packets per second, although the distance gap decreases as the order α increases, the values of the distance gap are still nonnegative, even when the order $\alpha = 10$. Second, for a given α, for example, $\alpha = 6$, the distance gaps between the legitimate traffic and the low-rate DDoS attacks have limited fluctuations with the increase of the packet rate, and these values are nonnegative as well. Therefore, we can see that the proposed measurement is effective in detecting these low-packet-rate DDoS attacks.

In addition to low-packet-rate attack, high-packet-rate attack is another challenge for the proposed measurement. We selected 10 datasets each for the legitimate traffic and the attack traffic, and the packet rates range from 10,000 packets per second to 100,000 packets per second. The reasons we chose these packet rates are that for the legitimate traffic, as we mentioned above, the rate of the packet size keeps increasing, and these selected rates generally represent the packet rates in real networks in recent years. As for the attack traffic, although these packet rates are greater than those of the original attacks, with the aim of achieving similarity with the legitimate traffic, the attacker may increase the packet rate to hide the attack. We evaluate formula (9) on these datasets, and the results are shown in Figures 18 and 19. The figures clearly show that the distance gaps are still nonnegative with the high packet rates. Therefore, the proposed measurement can detect low-rate DDoS attacks with high packet rates.

In summary, it has been demonstrated that the proposed measurement is effective in detecting low-rate DDoS attacks. First, the proposed measurement can detect the attacks not only in short terms but also in long terms since, in both cases, the distance gaps of the packet size between the legitimate traffic and the attack traffic are nonnegative for the appropriate α. Second, it is a stable measurement because the proposed measurement can distinguish between legitimate traffic and attack traffic with both low packet rates and high packet rates.

4.2. The Accuracy of the Proposed Measurement. In this section, we evaluate the accuracy of the proposed measurement. It is true that, for anomaly detection, the distance gap between the attack packets and the legitimate packets should

be expanded as much as possible to increase the detection sensitivity. However, it should be noted that the distance gap of our proposed measurement decreases with the increase of the order α. This is due to the balance between the distance gap and the false-negative rate.

The false-negative rate (R_{FN}) is determined by the relationship between the distance gap and the ratio of the low-rate attack packets based on EPSV. In this study, the false-negative rate is used to measure the ratio of the low-rate DDoS attack packets overflowed by EPSV, and it can be inversely reflected by the ratio of the low-rate DDoS attack packets based on EPSV, R_{EPSV}. The false-negative rate is $R_{\mathrm{FN}} = 1 - P_{\mathrm{EPSV}}$. Therefore, the larger P_{EPSV} is, the smaller R_{FN} is. In addition, for the aim of achieving a low false-negative rate, we should increase the order α since P_{EPSV} increases accordingly, as shown in Table 4, while the distance gaps and the false-negative rates decrease. As a result, the decrease of the distance gap is the result of achieving a balance between the distance gap and the false-negative rate, as they all decrease as α increases. Moreover, the choice of α is a compromise between making the distance gap large to improve the detection sensitivity and making the false-negative rate small to improve the detection accuracy. Therefore, four simulations regarding the relationship between the ratio of the distance gap (R_D) and the false-negative rates (R_{FN}) at various values of the order α are depicted in Table 5. The ratio of the distance gap (R_D), which is the ratio between the distance gap and the EPS of the attack traffic, is used to measure the degree to which the EPS of the legitimate traffic is greater than that of the attack traffic. It is calculated as $R_D = D(\alpha, \Delta t)/EPS(A)$. In Table 5, it is clearly observed that as α increases, the ratio of the distance gap and the false-negative rate decreases significantly. Table 5 indicates that the false-negative rates are quite low and decrease with increasing α, and some of them are even 0 when, for example, $\alpha > 3$. Second, when $\alpha = 0$, the false-negative rates of the two attacks are very large; that is, the proposed measurement might have a high false-negative rate if it does not consider the fluctuation of the attack-packet size; this is the key reason that the packet size of the attack is measured by EPSV instead of the EPS. Third, we should note that although the decreasing distance gap reduces the detection sensitivity, the proposed measurement is still effective, as the ratios of the distance gap are nonnegative and most of them have large values when α is chosen appropriately, for example, $2 \leq \alpha \leq 6$. However, as we mentioned above, the EPSV increases progressively with α, which causes the distance gap to decrease. We suggest that the choice of α should not too large. As a preset value of the detection, we believe that $\alpha = 6$ is a good choice for two reasons. First, while $\alpha = 6$, the EPSV of the attack traffics can cover at least 98.7% attack packets and therefore, the ratios of false negative are smaller than 1.3%. Second, the detection measurement is effective when $\alpha = 6$ as the ratios of the distance gap range from 486.45% to 655.41%, which are far greater than 0.

To sum up, the false-negative rate of the proposed measurement not only is low but also can be adjusted according to different requirements of the distance gap and false-negative rate.

5. Related Work

The recent work in this area can be divided into two categories: anomaly-based detection methods and signature-based detection methods. In anomaly-based detection, Zhang et al. [21] proposed a congestion-participation rate (CPR) metric and a CPR-based approach to detect and filter low-rate DDoS attacks. They found that low-rate DDoS flows actively induce network congestion, whereas normal TCP flows actively avoid network congestion. The proposed method was designed to distinguish attack flows from legitimate flows. However, more experiments and analyses using real datasets are needed to test its effectiveness.

Jadhav and Patil [22] proposed an optimal objective entropy based method to detect low-rate DDoS attacks. This approach is a considerable improvement over the traditional entropy metric. However, the distance value between normal traffic and attack traffic is quite small and therefore, the false-positive rate is large.

Xiang et al. [8] proposed a generalized entropy and information distance to detect and traceback low-rate DDoS attacks. Based on the generalized entropy distance between the legitimate traffic and the low-rate DDoS attacks, the proposed measurement outperforms the tradition Shannon entropy in terms of false-positive rate and distance gap. Although the distance gap can be adjusted by changing α, the distance gap is still small.

Similar to Xiang et al. [8], Bhuyan et al. [23] proposed a lightweight extended-entropy metric-based system for DDoS attack detection and IP traceback. The extended-entropy metric is an improvement of the generalized entropy in [8] to achieve a relatively greater distance than Yang's metric. However, the distance is still small due to the inherent limitation of entropy.

Du and Abe [24] proposed an IP packet size entropy metric to detect both long-term low-rate DDoS attacks and short-term high-rate DDoS attacks. Based on the assumption that many applications have typical packet sizes with respect to requests for and responses to data and acknowledgments, they claimed that the distribution of the packet size changes under attacks; this can be used to identify attacks to some degree. However, as the proposed method heavily relies on the packets in the observation window, this approach is limited in its scalability, and a long detection time is needed to achieve a high detection probability when suffering from a low-rate DDoS attack.

In the signature-based detection, Sun et al. [9] presented a distributed detection mechanism that uses the dynamic time-warping method to detect low-rate DDoS attacks. Based on the signature of the low-rate DDoS attack of a periodic short burst, they calculated the cumulative distance of the dynamic time warping between sampled flows and the template flows. The cumulative distance of the dynamic time warping indicates the similarity degree between the two flows. However, as it is based on the periodicity of the attack flow, in theory, it may be vulnerable in real networks and under unknown signature patterns.

Luo et al. [11] proposed a mathematical model to evaluate the combined impact of attack pattern and network

Table 5: The ratios of the distance and the ratios of the false-negative rate in different attack scenarios.

α	T = 30 s				T = 5 mins				R = 200				R = 20000			
	Constant		Pulsing		Constant		Pulsing		Constant		Pulsing		Constant		Pulsing	
	R_D (%)	R_{FN} (%)	R_D (%)	R_{FN} (%)	R_D (%)	R_{FN} (%)	R_D (%)	R_{FN} (%)	R_D (%)	R_{FN} (%)	R_D (%)	R_{FN} (%)	R_D (%)	R_{FN} (%)	R_D (%)	R_{FN} (%)
0	875.60	10.48	651.83	93.43	928.64	10.83	705.61	93.88	793.20	22.5	585.18	89.50	880.23	12.28	676.47	0
1	812.19	3.13	647.36	0.02	861.90	3.83	694.48	0.04	744.98	2	580.64	0	814.60	4.74	672.96	0
2	748.79	1.91	642.89	0.02	795.16	2.29	683.35	0.04	696.76	2	576.10	0	748.97	2.28	669.45	0
3	685.38	1.22	638.43	0	728.42	1.42	672.21	0.04	648.53	2	571.56	0	683.34	1.47	665.94	0
4	621.98	1.22	633.96	0	661.68	1.35	661.08	0.04	600.31	1	567.02	0	617.71	1.38	662.43	0
5	558.57	1.22	629.50	0	594.94	1.29	649.95	0.04	552.09	1	562.48	0	552.08	1.33	658.92	0
6	495.17	1.22	625.03	0	528.20	1.25	638.81	0.04	503.86	0.5	557.94	0	486.45	1.27	655.41	0
7	431.77	1.22	620.56	0	461.46	1.25	627.68	0.04	455.64	0.5	553.40	0	420.82	1.27	651.91	0
8	368.36	1.22	616.10	0	394.72	1.22	616.55	0.04	407.42	0.5	548.86	0	355.19	1.23	648.40	0
9	304.96	0.06	611.63	0	327.98	0	605.41	0.04	359.19	0.5	544.32	0	289.56	0	644.89	0
10	241.55	0.06	607.17	0	261.24	0	594.28	0.04	310.97	0.5	539.78	0	223.93	0	641.38	0

environment. They analyzed the vulnerability of a system to sophisticated attack and the model of the minimum transmission rate of attack packets to tune the attack effect. Although the proposed model uncovers some novel properties of low-rate DDoS attacks, more experiments using real datasets are needed to test their model.

Shevtekar et al. [25] proposed a lightweight data structure of packet arrival times at edge routers to detect low-rate DDoS attacks. A flow meeting two conditions, namely, the burst length is greater than or equal to the RTT and the time period is equal to the fixed minimum RTO, is marked as malicious by their method. However, they did not consider the network delay caused by network congestion, especially when a low-rate DDoS attack is ongoing, and tested the performance only using simulation data.

6. Summary and Future Work

In this paper, we propose a low-rate DDoS attack-detection measurement based on expectation of packet size. First, the experimental results with real datasets chosen from different times show that the EPS of the legitimate traffic is stable and large. Second, two typical low-rate DDoS attacks are simulated to demonstrate that the packet sizes of the attacks are quite small and limited, as measured by the EPS. Therefore, the distance gaps between the EPS of the legitimate traffic and EPSV of the attacks traffic samples can be used to identify a stable difference. Based on this difference, the proposed measurement can detect low-rate DDoS attacks, as was tested on real datasets. Furthermore, simulations of the distance gap have clearly demonstrated that the proposed approach is effective in both short-term and long-term detection and for both low packet rates and high packet rates. Particularly, the proposed approach can adjust the false-negative rate and the distance gap by adjusting the value of α. In conclusion, the proposed measurement can effectively detect low-rate DDoS attacks. In the next step, we plan to investigate and analyze the packet-size pattern of low-rate DDoS attacks, hoping to achieve a collaborative detection with the proposed measurement.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61350001) and National Pillar Program during the 12th Five-Year Plan Period (no. 2011BAD24B03-3).

References

[1] "Share of largest ddos attack defense combat in internet," 2015, http://www.infoq.com/cn/presentations/share-of-internet-world-largest-ddos-attack-defense-combat.

[2] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[3] S. Yu, Y. Tian, S. Guo, and D. O. Wu, "Can we beat DDoS attacks in clouds?" *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2245–2254, 2014.

[4] M. Sachdeva, K. Kumar, G. Singh, and K. Singh, "Performance analysis of web service under DDoS attacks," in *Proceedings of the 2009 IEEE International Advance Computing Conference, IACC 2009*, pp. 1002–1007, March 2009.

[5] M. Sachdeva and K. Kumar, "A traffic cluster entropy based approach to distinguish DDoS attacks from flash event using DETER testbed," *ISRN Communications and Networking*, vol. 2014, Article ID 259831, 15 pages, 2014.

[6] Y. Chen, S. Das, P. Dhar, A. El-Saddik, and A. Nayak, "Detecting and preventing ip-spoofed distributed dos attacks," *IJ Network Security*, vol. 7, no. 1, pp. 69–80, 2008.

[7] W. Zhou, W. Jia, S. Wen, Y. Xiang, and W. Zhou, "Detection and defense of application-layer DDoS attacks in backbone web traffic," *Future Generation Computer Systems*, vol. 38, pp. 36–46, 2014.

[8] Y. Xiang, K. Li, and W. Zhou, "Low-rate DDoS attacks detection and traceback by using new information metrics," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 426–437, 2011.

[9] H. Sun, J. C. S. Lu, and D. K. Y. Yau, "Defending against low-rate TCP attacks: Dynamic detection and protection," in *Proceedings of the 12th IEEE International Conference on Network Protocols, ICNP 2004*, pp. 196–205, October 2004.

[10] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks," in *Proceedings of the the 2003 conference*, p. 75, Karlsruhe, Germany, August 2003.

[11] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1069–1083, 2014.

[12] M. Sachdeva, K. Kumar, and G. Singh, "A comprehensive approach to discriminate DDoS attacks from flash events," *Journal of Information Security and Applications*, vol. 26, pp. 8–22, 2016.

[13] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1073–1080, 2012.

[14] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS attacks using entropy variations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 3, pp. 412–425, 2012.

[15] F. Liu, X. Wu, W. Li, and X. Liu, "The packet size distribution patterns of the typical internet applications," in *Proceedings of the 3rd IEEE International Conference on Network Infrastructure and Digital Content, IC-NIDC 2012*, pp. 325–332, September 2012.

[16] T. Thapngam, S. Yu, W. Zhou, and S. K. Makki, "Distributed Denial of Service (DDoS) detection by traffic pattern analysis," *Peer-to-Peer Networking and Applications*, vol. 7, no. 4, pp. 346–358, 2014.

[17] "Wide-transit 100 megabit ethernet trace 2007-01-09," 2007, http://imdc.datcat.org/collection/1-055M-0=WIDE-TRANSIT+100+Megabit+Ethernet+Trace+2007-01-09+.

[18] Widely Integrated Distributed Environment (Wide), http://www.wide.ad.jp/.

[19] "A day in the life of the internet," http://www.caida.org/projects/ditl/.

[20] "Center for applied internet data analysis," http://www.caida.org/data/passive/backscatter_dataset.xml.

[21] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, "Flow level detection and filtering of low-rate DDoS," *Computer Networks*, vol. 56, no. 15, pp. 3417–3431, 2012.

[22] P. N.Jadhav and B. M. Patil, "Low-rate DDOS Attack Detection using Optimal Objective Entropy Method," *International Journal of Computer Applications*, vol. 78, no. 3, pp. 33–38, 2013.

[23] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric," *Security and Communication Networks*, vol. 9, no. 16, pp. 3251–3270, 2016.

[24] P. Du and S. Abe, "IP packet size entropy-based scheme for detection of DoS/DDoS attacks," *IEICE Transaction on Information and Systems*, vol. E91-D, no. 5, pp. 1274–1281, 2008.

[25] A. Shevtekar, K. Anantharam, and N. Ansari, "Low rate TCP denial-of-service attack detection at edge routers," *IEEE Communications Letters*, vol. 9, no. 4, pp. 363–365, 2005.