Arabian Journal for Science and Engineering (2018) 43:7923–7931
https://doi.org/10.1007/s13369-018-3236-9

RESEARCH ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE

Two-Layer Approach for Mixed High-Rate and Low-Rate Distributed Denial of Service (DDoS) Attack Detection and Filtering

S. Toklu[1] · M. Şimşek[1]

Received: 28 July 2017 / Accepted: 26 March 2018 / Published online: 13 April 2018

Abstract
Distributed denial of service (DDoS) attacks are one of the most important attacks due to reducing the performance of computer networks nowadays. In recent years, the number of devices connected to the internet has been increasing. These devices are not only computers, but also objects of everyday use. The concept of internet has accelerated the increase considerably. Therefore, many problems arise in terms of DDoS attacks. One of them is low-rate DDoS attacks. While high-rate DDoS attacks are often performed with computers, low-rate DDoS attacks can be easily performed by computers and internet-connected objects. Therefore, effective defense mechanism against both attacks must be developed. In this study, new approaches are proposed to filter mixed high-rate DDoS and low-rate DDoS attacks. The ns-2 simulation tool was used to evaluate the performance of the proposed methods. Experimental results show that the proposed methods are successfully filtered mixed DDoS attacks.

Keywords Network-level security and protection · Security · Distributed denial of service attacks · QoS · Intrusion detection system

1 Introduction

Distributed denial of service (DDoS) attacks create serious problem for internet services by using a group of connected devices as an attacker. Attackers using DDoS attacks try to reach innocent computers for their attack. Such attacks cause to consume the resources of a server or a router. Depletion of resources prevents legitimate users to use the resources. Also, the bandwidth of the network is consumed. DDoS attacks are large-scale attacks in distributed collaboration that can be done on all networks. Service providers want to defend their networks against DDoS attacks [1]. They want to ensure that legitimate users have uninterrupted access. However, it is difficult to separate which attack traffic is legitimate or DDos attacks because such attacks are similar to legitimate traffic generally.

✉ S. Toklu
sinantoklu@duzce.edu.tr

M. Şimşek
mehmetsimsek@duzce.edu.tr

[1] Department of Computer Engineering, Faculty of Engineering, Düzce University, Konuralp Campus, 81620 Düzce, Turkey

Two types of traffic are usually used in DDoS attacks. These are named as high-rate DDoS attack traffic and low-rate DDoS attack traffic. High-rate DDoS attacks cause unusual and instantaneous growth in high-rate DDoS attack traffic. On the other hand, low-rate DDoS attack traffic is generally similar to legitimate traffic. It is difficult to identify DDoS attacks in a situation similar to legitimate traffic [2]. The purpose of recent field trials is to identify especially DDoS attacks. It is initiated by botnets. A botnet is established in a large network with many open devices. Detection of the botnets is difficult and an effective solution for the attacks. In short, the monitoring of all machines that may be active bots in the botnet is a solution for system [3]. At the same time, detection of high-rate and low-rate DDoS attacks is difficult. Especially, since low-rate DDoS attack traffic resembles legitimate traffic, it is difficult to detect these type of attacks [4].

According to our literature review, there are two main metrics used to detect DDoS attacks. These are: metric1—Counting the packets on the queue of the victim router at small time intervals and transforming it into a signal; metric2—Recording the differences between the arrival times of the packets to the victim router and transforming into a signal. The metric1 is widely used in the literature such as studies [5–7]. The metric2 is used in [8].

We developed a two-layer filtering approach that can detect both high-rate and low-rate attacks. One of them, average filter with the metric1 to detect high-rate DDoS attacks. Second, discrete Fourier transform (DFT) with the metric2 to detect low-rate DDoS attacks.

Our contributions are summarized as follows:

- The proposed methods are easy to implement.
- The proposed methods detect high and low-rate DDoS attacks at the same time.
- We used DFT to analyze the differences between the arrival times from the packets to the victim router.
- The proposed methods have zero false-positive and false-negative rates under the current scenarios.
- The proposed methods detect the attacks in a few seconds.

The remainder of the paper is organized as follows: In Sect. 2, the related works are presented. The proposed methods are described in Sect. 3. Section 4 gives materials and methods used in the study. Experimental results are explained in Sect. 5. Various important points are considered and discussed in the paper. Also, the paper is summarized in Sect. 6.

2 Related Works

Essentially, DDoS filtering is a pattern recognition and classification problem. A number of studies have been conducted in the area of defense methods and strategies against DDoS attacks. The source-side defense mechanism of those who use them is to determine and stop DDoS attacks at the source. The purpose of the mechanism is to block the attack on the side of the attacker. In this respect, the victim host is aimed to be rescued from this attack with minimum damage [8,9].

In [10], the authors mentioned that there is a similarity between attackers. A detection system called partial rank correlation-based detection (PRCD) was proposed because of this similarity. In [11], LDDoS attacks resemble small periodic signal pulses, and TCP flows resemble background noise. In addition, this study shows that Chaos systems are sensitive to deterministic signals such as periodic LDoS attacks. In [8], a new metric has been proposed named as mean inter-packet delay variation (mipdv) to distinguish LDDoS attacks from benign TCP flows. This approach considers the repetition interval of LDDoS attacks.

In the victim-side detection/filtering methods, detection and filtering are performed on the victim's hosted network. One of the problems is that the sources of the victim become unusable during DDoS attacks. Another problem is that the attack can only be detected after reaching the victim. In this case, the detection of the attack is not very meaningful since legitimate traffic is largely blocked [12]. In [7], data flows are classified according to their behavior in case of congestion. If a flow causes congestion, it is classified as an attacker. For this, the packet queue of the router is monitored periodically. In [4], a lot of information metrics are examined for LDDoS detection. Each metric examined is for determining the attack pattern. In the study, network flow was sampled between 5 min and 10 s. For the detailed mathematical analysis of LDDoS attacks, the study in [13] can be examined. In a study, LDDoS bots were replicated for multi-target attack scenarios [14]. Bots are used to attack other targets in the free time of the mount. In this way, the ability of a botnet to attack is being developed. In another study, the attack duration is adjusted to the time that the router's buffer is full [15]. Therefore, TCP is damaged significantly with short attack periods. In a study similar to this situation, attack periods are adjusted according to TCP behavior [16]. During the slow start phase of TCP, attackers are starting a new attack. So the victim's buffer is congested. In addition to the above-mentioned general methods, many theoretical-based metrics have been proposed to overcome the problems encountered by DDoS attack detection methods. In [17], chaotic-based model has been presented. This model tries to differentiate legitimate traffic with DDoS attack using network similarity theory. Another study in [18] offers a cooperative early detection system. In this system, flooding attacks which are very far to the target is detected at ISP level. It provides a distributed deployment architecture consisting of multiple ISPs that form a network. In [19], the authors present an independent DDoS attack detection method and attempt to detect the attack at an early stage. In another study, DDOS uses variants of lyapunov exponent with low false-positive rate to detect attack traffic [20]. The entropies of the source IPs estimate the target IPs at each unit time and detect the exposures via the exponent separation rate. In another study, a metric named mean inter-packet delay variation (mipdv) was proposed which calculates the order of difference for arrival times of IP packets sent by aggressive devices to the victim device [8]. With this metric, attack can be detected at flow level.

In the literature, there are also many studies about signal processing methods are used to detect DDoS. In [5], discrete Fourier transform (DFT) and discrete wavelet transform (DWT) are used to detect attacks. The authors have sampled the number of packets with 1 ms intervals. Then, DFT and DWT are applied to the obtained samples. Finally, attacks and normal traffic are distinguished with using a Naive Bayes Classifier. Also in [6], DFT is used to detect attack traffic. The authors have sampled the number of packets with 1 ms intervals. If there is a pattern in all samples, this means that the pattern is created by attackers. So, problem is induced to a pattern recognition problem.

According to our literature review, there is no study to detect low- and high-rate DDoS attacks at the same time. The tools used by the attackers are becoming more diverse and

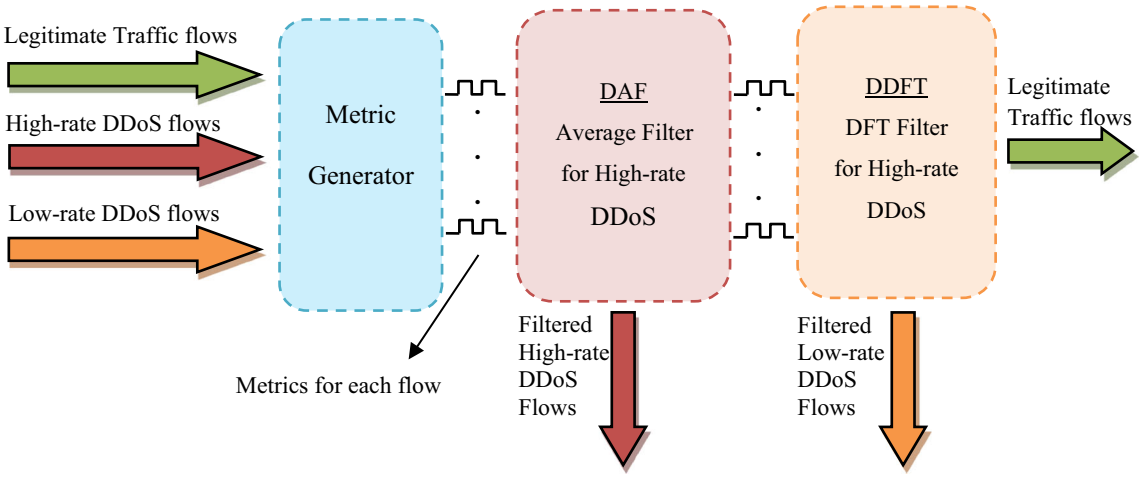

Fig. 1 The overall structure of the proposed two-layer approach

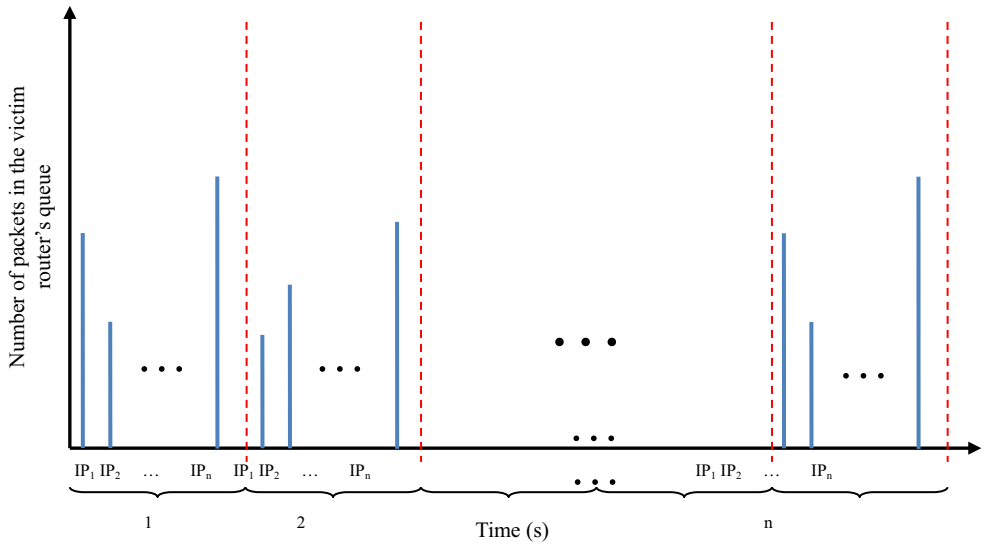

Fig. 2 Sampling victim router queue for a period of time

more complex day by day. Attackers can use low- and high-rate attacks in a single attack. In this context, it is important that these two types of attacks be identified at the same time. The aim of this study is to detect low- and high-rate attacks at the same time, fast and with high accuracy.

3 The Proposed Methods

High-rate and low-rate DDoS attacks have different characteristics. So it is difficult to develop a unique approach to detection. In this study, we proposed a two-layer filtering method for mixed DDoS attacks. The overall structure of the developed system is shown in Fig. 1. The first stage of the system is the extraction of metric1 and metric2 for all incoming flows. After that, all flows' metrics are passed to DAF (detection with average filter) unit. DAF filters High-rate DDoS attack flows. Then, DAF passes remaining flows' metrics to DDFT (detection with discrete Fourier transform) unit. Finally, DDFT filters Low-rate DDoS attack flows and passes legitimate traffic flows.

In order to detect high-rate DDoS attacks, we counted the packets in the router's queue when the victim router is congested with one second intervals and we classified the packets according to source IPs. So, we obtained the metric1. This can be likened to take a photo of the router queue with 1-s exposure time. So, we got information about how many packets from which IP source in each photo. This situation is shown in Fig. 2. In the figure, n photos of the router queue are shown. A benign TCP source reduces its rate in the congestion. However, an attacker does not change its rate. This causes attacker IP sources to be constant in the queue photo received during

congestion and also causes benign TCP sources to appear at different rates in different photos. If we look at the signal processing perspective, we can think the attack traffic as signal and TCP traffic as noise.

```
Algorithm 1. Detection with Average Filter
DAF()
Define SamplingNumber as integer
n=0
while there is congestion do
{Count packets for each IP source with 1 s interval
Match each IP with a number i}
        P[n][i] = P[n][i]+1
        n=n+1
        if congestion is over or n> SamplingNumber then
                break
        end if
end while
{Calculate total packets for each IP source and calculate overall
number of packets}
for each i in IP list
for j=0 to n-1 do
Total_Packets_Per_IP[i]=Total_Packets_Per_IP [i] + P[j][i]
end for
Total_Packets=Total_Packets+Total_Packets_Per_IP[i]
{Calculate averages}
Average_Per_IP[i]=Total_Packets_Per_IP[i] /(n-1)
Average_For_All_IPs = Total_Packets /(n-1)
end for
{Decision stage}
for each i in IP list
        if Average_Per_IP[i] > Average_For_All_IPs then
                Categorize IP source i as an attacker
        end if
end for
```

Basically, if we can separate the signal and the noise, we separate the attacker and the benign TCP as well. For this purpose, we have applied an average filter to the captured queue photos to determine which IPs are in all the photos. Thus, we distinguish attack traffic from benign TCP. The algorithm that is developed to detect high-rate DDoS, named as detection with average filter (DAF) is shown in Algorithm 1. In Algorithm 1, *SamplingNumber* is the maximum number of samples taking by 1 s intervals; matrix P keeps total number of packets for each IP sources. P's raws indicate samples and P's columns indicate IP sources. In low-rate DDoS attacks, the average values of attacker packets and legitimate flows' packets calculated in Algorithm 1 are getting closer to each other. So, low-rate DDoS attacks cannot be detected with Algorithm 1. However, the LDDoS attack packets have a pattern of arrival times to the victim router. An example for this pattern is shown in Fig. 3. In fact, the difference for the arrival times of low-rate DDoS attack packets by the victim router indicates a certain oscillation. On the other hand, benign TCP packets do not have a specific oscillation. If this oscillation can be detected, Low-rate DDoS can be detected. For this purpose, we recorded the differences between the arrival times of the packets in the victim router queue for a certain period of time according to their sources during the time of the congestion like in [8] and we obtained the metric2. Let $\Phi = \{\varphi_0, \ldots, \varphi_n\}$ be a flow, where n is total packet number and $P = \{\rho_0, \ldots, \rho_n\}$ be receiving times of the packets of Φ, and $\Theta = \{\theta_0, \ldots, \theta_{n-1}\}$ be the difference between the reception times of the packets where $\theta = \{\rho_1 - \rho_0, \ldots, \rho_n - \rho_{n-1}\}$. In [8], mean values of Θ named as *mipdv* were used to filter LDDoS attacks. Instead of *mipdv*, we calculated the oscillation amplitude for each IP source by applying discrete Fourier transform (DFT) to Θ and we get $\mathcal{F}(\Theta) = \{\mathcal{F}(\theta_0), \ldots, \mathcal{F}(\theta_j)\}$. The general formula of DFT is given in (1).

$$X[k] = \sum_{0}^{N-1} x[n]\, e^{\frac{-j2\pi kn}{N}} \tag{1}$$

Here x denotes Θ; X denotes $\mathcal{F}(\Theta)$. The result obtained with DFT shows a large difference for attacker sources and

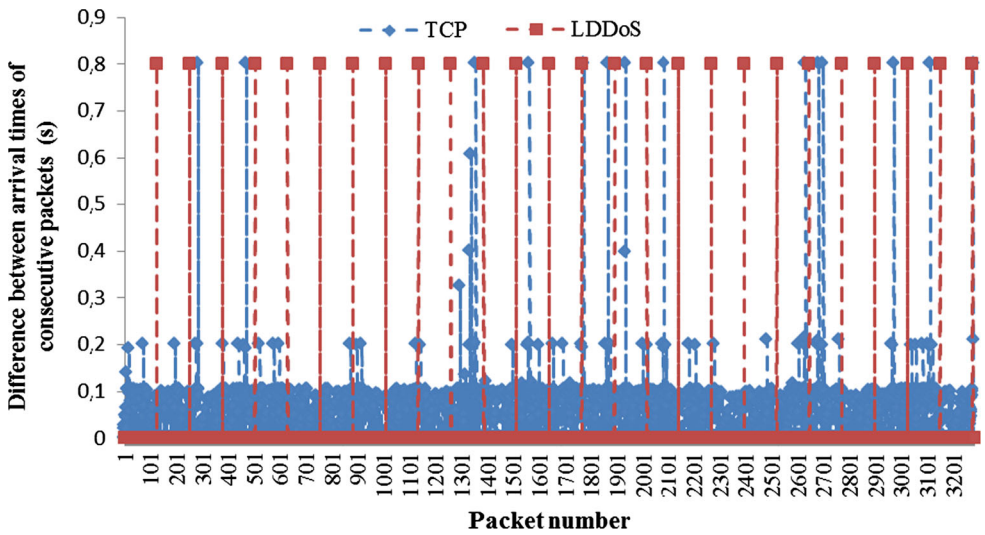

Fig. 3 The differences between arrival times of packets to victim router under low-rate DDoS

benign TCP sources. If a certain number of samples (T) have exceeded the predetermined threshold amplitude value (τ), we decide that this source is an attacker. The formulation of this comparison is given in (2).

$$T \geq \sum_{j=0}^{n} \begin{Bmatrix} 0 \\ 1 \end{Bmatrix} \begin{vmatrix} \mathcal{F}(\theta_j) < \tau \\ \mathcal{F}(\theta_j) \geq \tau \end{vmatrix} \tag{2}$$

Here n donates length of $\mathcal{F}(\Theta)$. If (2) is fulfilled for an i which is $i \in I$, I is the IP addresses set; i is marked as an attacker. We specified τ and T as variable. τ should be selected base on the attack's data rate. For higher attack data rates, τ should be selected smaller because of the amplitude of attack will be smaller. For lower attack data rates, τ should be selected larger because of the same reason. T is directly related with observation time. For higher observation times T can be selected larger. In our simulation empirically, we selected τ as 15 and T as 5. We named this method as detection with discrete Fourier transform (DDFT). DDFT algorithm is shown in Algorithm 2. Here, we must say that, in high-rate DDoS attacks, the difference between the reception times of attack packets does not show a pattern like this. For this reason, the use of DFT in detecting high-rate DDoS is not beneficial. An example pattern of arrival times of high-rate DDoS attack packets to the victim router is shown in Fig. 4.

In Algorithm 2, *SamplingDuration* is the time for taking samples; *Threshold* is predetermined amplitude threshold; *SampleNumberThreshold* is number of samples have exceeded the predetermined amplitude threshold; matrix *Times* keeps receiving times of the packets for each IP source. The *Times'* raws indicate IP sources and *Times'* columns indicate samples.

Algorithm 2. Detection with Discrete Fourier Transform

```
DDFT()
Define SamplingDuration as Time
Define Threshold as Float
Define SampleNumberThreshold as Integer
n=0
while there is congestion and SamplingDuration is not over
do
        {Keep packets receiving times for each source
        Match each IP with a number i}
        Times[i][t] = Receiving_time_of_packet;
        t=t+1
end while
{Calculate the differences between the reception times of the packets
for each IP source }
for each i in IP list
for j=1 to t do
Time_Differences_Per_IP[i] = Times[i][j] – Times[j][t-1]
end for
{Applying Discrete Fourier Transform}
Times_DFT_Result[i] = DFT(Time_Differences_Per_IP[i])
end for
{Decision stage}
for each i in IP list
        for j=0 to t-1 do
        if Times_DFT_Result[i][j] > Threshold
                SampleNumber = SampleNumber + 1
        end if
        if SampleNumber > SampleNumberThreshold
                Categorize IP source i as an attacker
                break
        end if
        end for
end for
DFT() with Array RETURNING Array
        {Discrete Fourier Transform Routines}
```

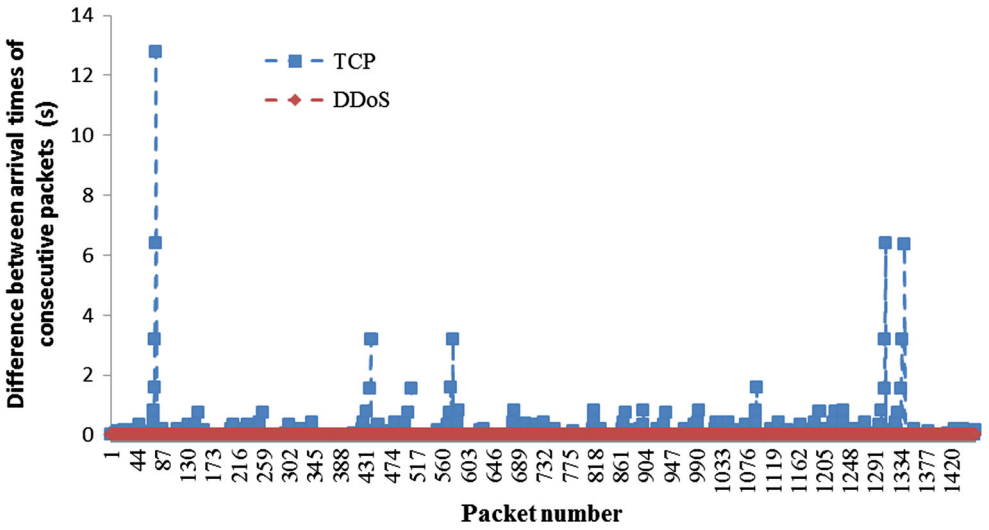

Fig. 4 The differences between arrival times of packets to victim router under high-rate DDoS

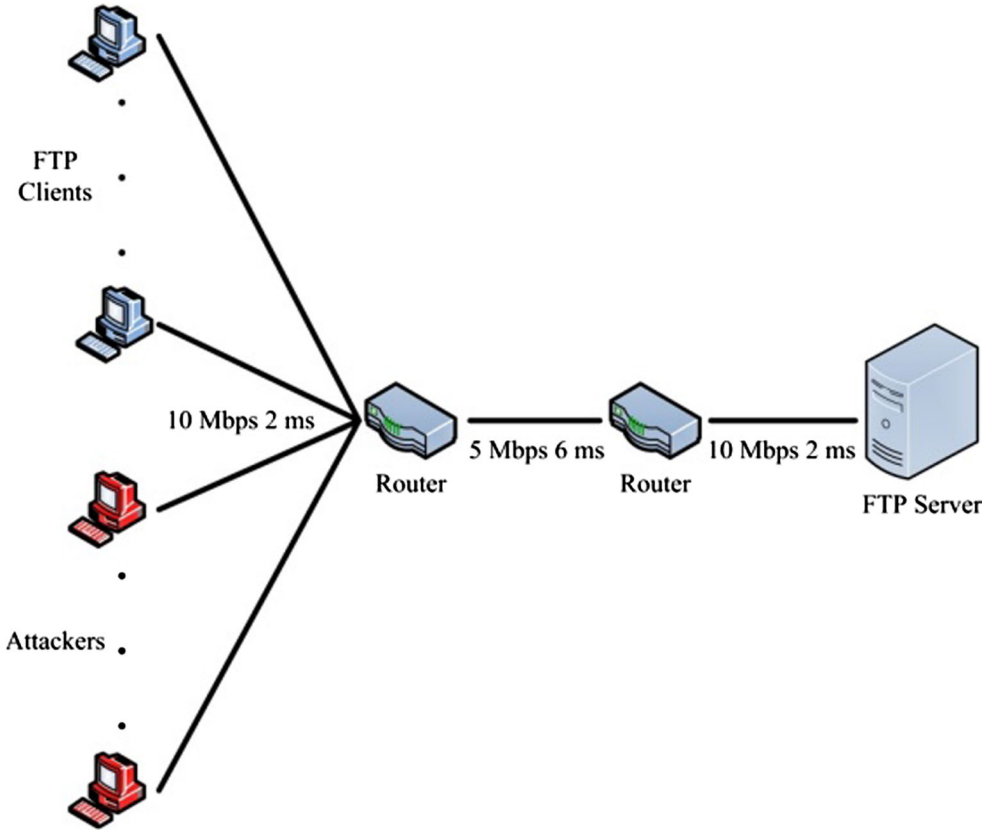

Fig. 5 The topology used in the simulations

4 Materials and Methods

We conducted a series of simulations with ns-2 to evaluate the proposed approach. The topology that is used in the simulations is shown in Fig. 5. It has 30 benign FTP over TCP users, 20 attackers, 2 routers and 1 server. Connection details are given in Fig. 5.

An LDDoS attack is defined with following parameters. T_{on}: The time (s) that an attacker generates attack packets; T_{off}: The time (s) that an attacker stops the attack; R: The rate of attack traffic (in bps). In the low-rate DDoS simulations, we set $T_{on} = 0.2$ s and $T_{off} = 0.8$ s. In high-rate DDoS simulations, attackers continuously send packets to the victim. Also we set $R = 0.25$ Mbps for both attack types. There are 20 attackers; so total attack traffic rate reaches to 5 Mbps which equals to the bandwidth between two routers. Actually, a high-rate DDoS attack may have a data rate greater than victim network's bandwidth.

5 Experimental Results

We tested DAF and DDFT methods with mixed High-rate and Low-rate attack scenarios and obtained the results. DAF results on the high-rate DDoS attacks are shown in Fig. 6. The scenario has been tested for 6 different sampling numbers (1, 5, 15, 30, 60, 120). The average value for legitimate traffic is around 9; attack traffic is around 623; the overall average is around 254. DAF can successfully distinguished legitimate traffic from attack.

Also, we tested DAF with low-rate DDoS. DAF results on the low-rate DDoS scenario are shown in Fig. 7. In the same way, the scenario has been tested for six different sampling numbers (1, 5, 15, 30, 60, 120). The average value for legitimate traffic is around 21; attack traffic is around 117; the overall average is around 59. As the data rates of the attackers decreased, the average values are converged. If the same total attack traffic rate is created with 100 attackers instead of 20; namely, if the traffic rate per attacker is 0.025 Mbps instead of 0.25 Mbps; the average values would be closer to each other. In this case, the DAF would not be able to distinguish legitimate and attack flows.

The differences between arrival times of consecutive packets in the low-rate DDoS scenario for one attacker and one legitimate user are shown in Fig. 8. Figure 9 shows that DFT is applied to these values. DDFT can successfully distinguish legitimate and attack flows.

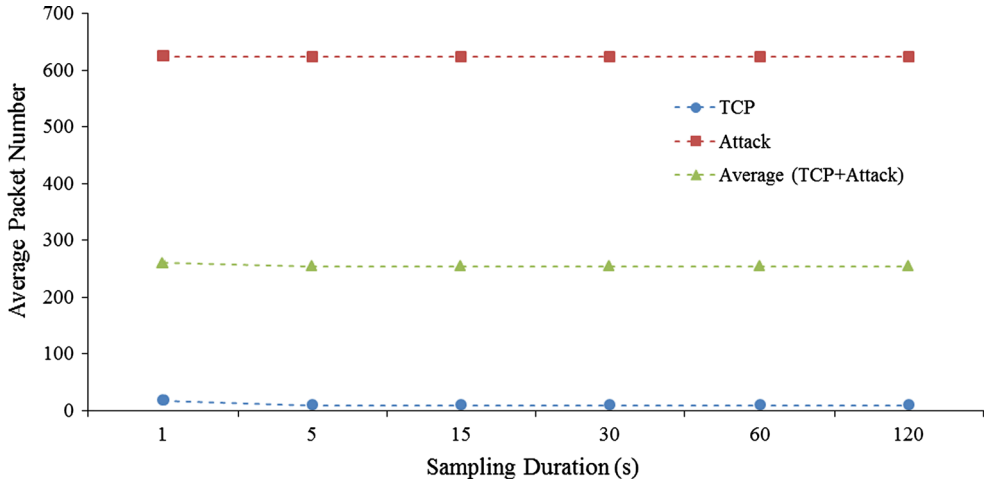

Fig. 6 DAF results on high-rate DDoS scenario

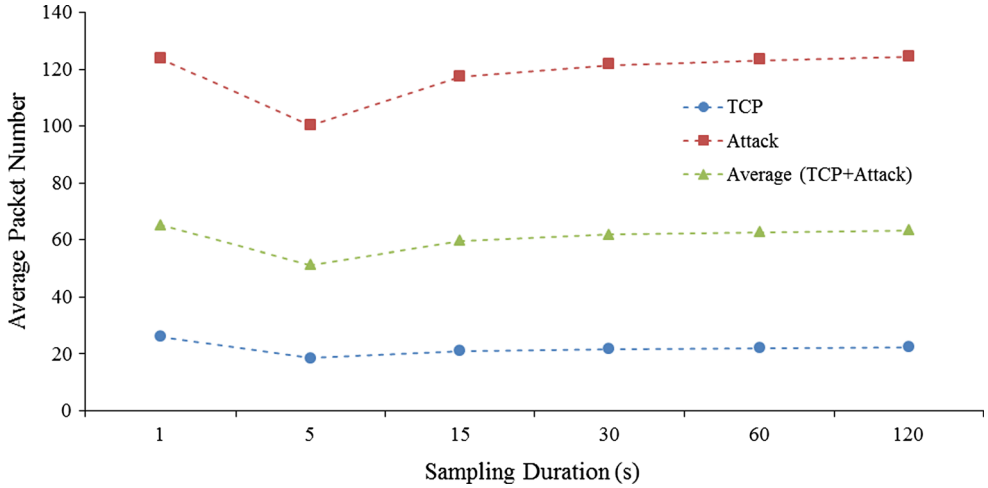

Fig. 7 DAF results on low-rate DDoS scenario

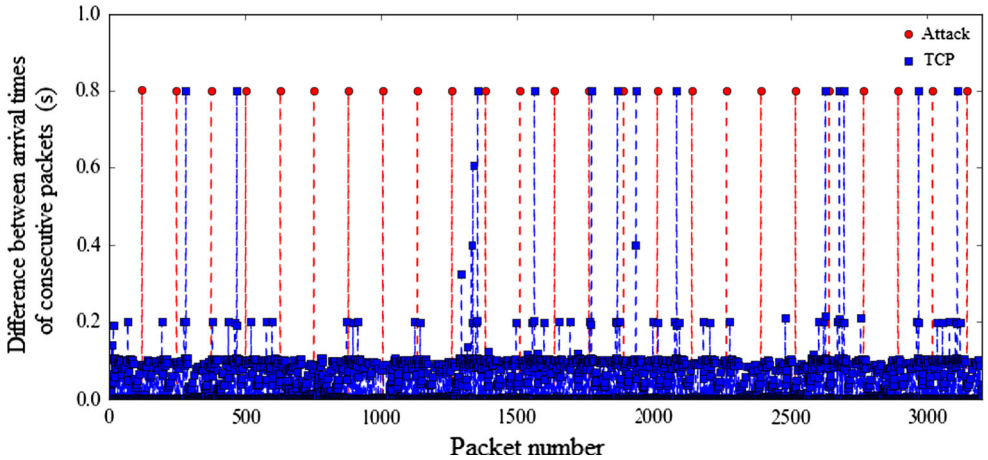

Fig. 8 The differences between arrival times of packets to victim router under low-rate DDoS

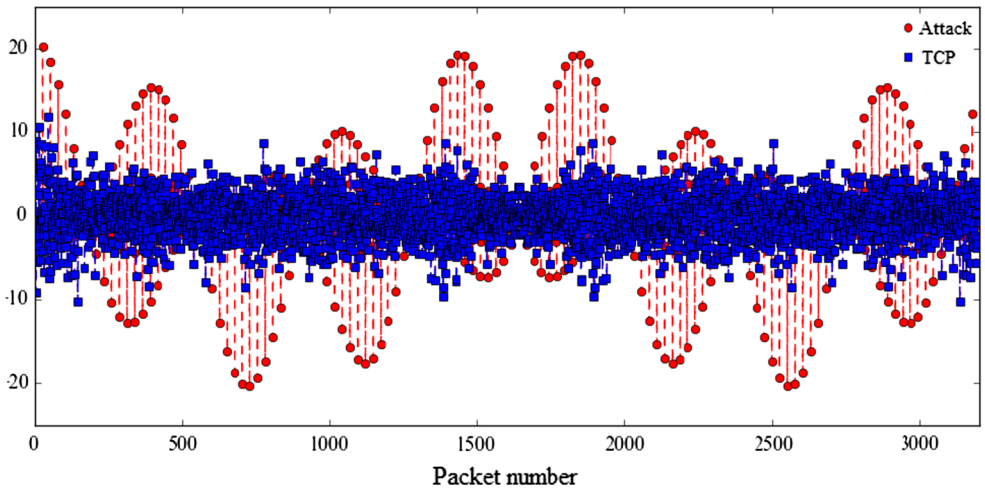

Fig. 9 DFT of the differences between arrival times of packets to victim router under low-rate DDoS

Also we tested DDFT with high-rate DDoS. Since the oscillation in the low-rate DDoS attack did not occur here, DDFT could not detect the high-rate DDoS attacks.

6 Discussion and Conclusion

The use of the metric2 described in Study 8 with the DFT gave better results than *mipdv*. According to the experimental results, DAF and DDFT successfully detect all (100%) high-rate and low-rate DDoS attackers in the scenarios. Also the used methods, namely, average filter and discrete Fourier transform are easy to design and implement.

However, there are some issues that need to solve. A situation where high-rate and low-rate attacks are close to each other will make the detection harder. Namely, as the line separating the two attack types becomes unclear, the accuracy rates of the detection methods will decrease. This is also a matter to be assessed.

To make the calculations (average filter and discrete Fourier transform), it is necessary to capture and store the sample at the proper amount for each IP. This is a problem if we have hundreds of thousands of attackers or normal users. For this reason, DAF and DDFT methods have to work on high performance devices. Also, since the attack detection process begins with the detection of the congestion state, this device needs to communicate with the victim router (or it must identify the congestion itself).

Since the proposed methods have zero false-positive and false-negative rates under the current scenarios, we did not compare these parameters with another method. However, the proposed methods are not the fast methods in the literature. In [8], with using *mipdv*, LDDoS attacks are detected in a few milliseconds with low (but not zero) false-positive and false-negative rates, whereas DDFT needs at least a few seconds to detect an attack.

Besides, it is a general problem to determine when an attack started. Each congestion state may not be caused by an attack. In this case, running attack detection and filtering systems will force us to filter out completely well-intentioned traffic.

References

1. Gui, L.; Zhou, Y.; Xu, R.; He, Y.; Lu, Q.: Learning representations from heterogeneous network for sentiment classification of product reviews. Knowl. Based Syst. **124**, 34–45 (2017)
2. Zhi-Jun, W.; Hai-Tao, Z.; Ming-Hua, W.; Bao-Song, P.: MSABMS-based approach of detecting LDoS attack. Comput. Secur. **31**(4), 402–417 (2012)
3. Ding, K.; Li, Y.; Quevedo, D.E.; Dey, S.; Shi, L.: A multi-channel transmission schedule for remote state estimation under DoS attacks. Automatica **78**, 194–201 (2017)
4. Bhuyan, M.H.; Bhattacharyya, D.K.; Kalita, J.K.: An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognit. Lett. **51**, 1–7 (2015)
5. Fouladi, R.F.; Kayatas, C.E.; Anarim, E.: Frequency based DDoS attack detection approach using naive Bayes classification, In: 2016 39th International Conference on Telecommunications and Signal Processing (TSP), pp. 104–107 (2016)
6. Chen, Y.; Hwang, K.: Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. J. Parallel Distrib. Comput. **66**(9), 1137–1151 (2006)
7. Zhang, C.; Cai, Z.; Chen, W.; Luo, X.; Yin, J.: Flow level detection and filtering of low-rate DDoS. Comput. Netw. **56**(15), 3417–3431 (2012)
8. Şimşek, M.: A new metric for flow-level filtering of low-rate DDoS attacks. Secur. Commun. Netw. **8**(18), 3815–3825 (2015)
9. Mirkovic, J.; Reiher, P.: D-WARD: a source-end defense against flooding denial-of-service attacks. IEEE Trans. Dependable Secur. Comput. **2**(3), 216–232 (2005)
10. Bhuyan, M.H.; Kalwar, A.; Goswami, A.; Bhattacharyya, D.K.; Kalita, J.K.: Low-rate and high-rate distributed DoS attack detection using partial rank correlation. In: Proceedings of 2015 5th

International Conference on Communications Systems and Network Technologies CSNT 2015, pp. 706–710 (2015)
11. Wu, Z.J.; Lei, J.; Yao, D.; Wang, M.H.; Musa, S.M.: Chaos-based detection of LDoS att acks. J. Syst. Softw. **86**(1), 211–221 (2013)
12. Shin, S.; Kim, K.; Jang, J.: D-SAT: Detecting SYN flooding attack by two-stage statistical approach. In: Proceedings of International on Symposium on Applications and Internet, pp. 430–436 (2005)
13. Luo, J.; Yang, X.; Wang, J.; Xu, J.; Sun, J.; Long, K.: On a mathematical model for low-rate shrew DDoS. IEEE Trans. Inf. Forensics Secur. **9**(7), 1069–1083 (2014)
14. Li, H.; Zhu, J.; Wang, Q.; Zhou, T.; Qiu, H.; Li, H.: LAAEM: a method to enhance LDoS attack. IEEE Commun. Lett. **20**(4), 708–711 (2016)
15. Yue, M.; Wu, Z.; Wang, M.: A new exploration of FB-shrew attack. IEEE Commun. Lett. **20**(10), 1987–1990 (2016)
16. Luo, J.; Yang, X.: The NewShrew attack: a new type of low-rate TCP-targeted DoS attack. In: IEEE International Conference on Communications (ICC), vol. 2014, pp. 713–718 (2014)
17. Chonka, A.; Singh, J.; Zhou, W.: Chaos theory based detection against network mimicking DDoS attacks. Communications **13**(9), 717–719 (2009)
18. François, J.; Aib, I.; Boutaba, R.: FireCol: A collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans Netw (TON) **20**(6), 1828–1841 (2012)
19. Tao, Y.; Yu, S.: DDoS attack detection at local area networks using information theoretical metrics. In: 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 233–240 (2013)
20. Ma, X.; Chen, Y.: DDoS detection method based on chaos analysis of network traffic entropy. IEEE Commun. Lett. **18**(1), 114–117 (2014)