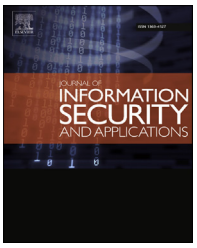
Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



A comprehensive approach to discriminate DDoS attacks from flash events

Monika Sachdeva [a,*], *Krishan Kumar* [a], *Gurvinder Singh* [b]

[a] *Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India*
[b] *Guru Nanak Dev University, Amritsar, Punjab, India*

ARTICLE INFO

Article history:
Available online 14 December 2015

Keywords:
Distributed denial of service (DDoS)
Flash event (FE)
Entropy
Receiver operating characteristic curve (ROC)

ABSTRACT

Most of the business applications on the Internet are dependent on web services for their transactions. Distributed denial of service (DDoS) attacks either degrade or completely disrupt web services by sending a flood of packets in the form of legitimate looking requests towards the victim web servers. Flash event (FE), which is an overload condition caused by a large number of legitimate requests, has similar characteristics as that of DDoS attacks. Therefore, detection of DDoS attacks with FE as background traffic is one of the hardest problems confronted by the network security researchers. Moreover, DDoS attacks and FEs require altogether different handling procedures. In this paper, traffic cluster entropy is derived from source address entropy and their combination is used not only to detect various types of DDoS attacks against web services but also to distinguish DDoS attacks from FEs. Optimal thresholds for traffic cluster entropy are calibrated through receiver operating characteristic curve (ROC). Proposed detection approach can operate in one of the defence modes: naive, normal or best, based on attack detection sensitivity requirements. Sensitivity of detection metric is tested using multiple simulation scenarios with different types of DDoS attacks along with variation in origins of attack and FE traffic. Detection of a variety of DDoS attacks like high rate skewed DDoS attacks, low rate isotropic attacks, subnet spoofed DDoS attacks and sophisticated DDoS attacks has been demonstrated. The effectiveness of the proposed approach in terms of false positive rate, detection rate and classification rate is validated through simulations carried out using NS-2 on a Linux platform.

1. Introduction

Distributed denial-of-service (DDoS) attacks have been wreaking havoc on the Internet and its services from approximately the last 12 years. Recent research from the Arbor Networks fifth annual Worldwide Infrastructure Security Report (McPherson et al., 2010) has shown that DDoS attacks are not only getting larger and more frequent, but also becoming more sophisticated as they pinpoint specific applications with smaller, more targeted and stealthy attacks. FE is a situation in which a large number of legitimate users simultaneously access a server causing traffic peaks which partially or sometimes completely disrupt the services. FE and DDoS attacks share a number of similar characteristics that make it difficult to distinguish between them (Jung et al., 2002). Both FE and DDoS are caused by a large number of client requests. The consequences of both FE and DDoS include slow responses and connection drops. In the case of FE and un-spoofed DDoS attacks, the difference only lies in user intention, which is hard

* *Corresponding author.* Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India. Tel.: +91 9463000845; fax: +91 1632 242138.
E-mail address: monika.sal@rediffmail.com (M. Sachdeva).

http://dx.doi.org/10.1016/j.jisa.2015.11.001

to detect at the victim's end. So, it is the intent rather than the content that has to be investigated carefully in order to discriminate between FEs and DDoS attacks. In case of FE, high volume of traffic generated in the form of legitimate requests need to be serviced by provisioning extra resources, but in case of DDoS attack, characterisation of attack traffic and then filtration are required to eliminate malicious traffic. Hence, it is important to discriminate them as both require altogether different mechanisms for their handling. The increased frequency as well as sophistication of DDoS attacks has made its defence a serious problem. The seriousness of the DDoS problem has led to the development of numerous detection and mitigation mechanisms. Although many solutions have been proposed, the problem is hardly tackled, let alone solved. Most of the work lacks testing in different attack scenarios especially FE as background traffic. Moreover, systematic procedure for setting thresholds is missing in the literature available in this area (Carl et al., 2006; Peng et al., 2007). Major contributions of this paper are:

- Traffic cluster entropy based approach has been proposed that not only detects DDoS attacks against web services but also distinguishes it from flash events with accuracy. The accuracy is measured in terms of false positive rate (FP_R), detection rate (D_R), and classification rate (C_R).
- This work involves formulation of detection model and calibration of thresholds using request operating characteristic (ROC) curves.
- Provision of adaptability in proposed detection model to operate in different modes based on QoS and security requirements of the service.
- In order to carry out comprehensive testing, design of simulation scenarios has been done using a variety of DDoS attacks and FE. Validation of traffic cluster entropy as a DDoS attack detection metric has been carried out on network simulation test bed NS-2.

The paper has been organised as follows:

Section 2 reviews the current available literature. Section 3 explains our proposed approach to detect DDoS attacks and to discriminate it from flash event. Design of simulation experiments is discussed in Section 4. Section 5 includes threshold calibration and results. Section 6 concludes our work with an insight to future plan.

2. Related work

The recent work in this area can be classified on the basis of probability distribution of traffic sources, web access patterns and automated nature of DDoS attack sources. The first two categories use anomaly based detection methods and the third category makes use of reverse Turing tests.

Anomaly based DDoS detection methods rely on identifying the unusual behaviour by comparing against the legitimate traffic models. Kumar et al. (2007), Sardana and Joshi (2009), and Gupta et al. (2012) have used anomaly based approach. These approaches however do not address flash events that have similar features as DDoS attacks. It is necessary to discriminate DDoS flooding attacks from flash events as attackers can imitate traffic features of a flash event so as to evade its detection. Chen et al. (2007) distinguish flash events from DDoS flows using the change point detection method. Zombies can increase the number of attack packets very slowly, which will surely escape the change point detectors. Yu et al. (2011) has used information distance to detect as well as distinguish DDoS attacks from FE but with low detection accuracy. Xie and Yu (2009) proposed a technique to detect application layer DDoS attacks and also to discriminate flash event from application based DDoS attacks (HTTP flood with valid TCP connections). The rationale is based on zipf-like distribution of document accessing popularity in web logs for normal and flash traffic. This distribution significantly varies from zipf-like distribution in case of DDoS attacks. It is seen that the entropy of document popularity remains in constant range without attack, i.e. normal and flash event, which however decreases under DDoS attack. The drawback of this approach is that the attacker can mimic zipf-like distribution by instructing the bots to send HTTP requests to the target web server and then parse the replies and follow hyperlinks recursively. Xie et al. (2013a) proposed HsMM based detection scheme for the attacks being redirected to the victim server by the use of web proxies. The authors identified the dominant/visible and recessive/invisible features of proxy-to-server aggregated traffic. The traffic directed towards the server is compared against this model to determine the judgement index that will be used for service acceptance or rejection decisions. Xie et al. (2013b) proposed a scheme that primarily detects web proxy based DDoS attacks using hidden semi Markov model. The authors captured temporal and spatial localities to model web proxies' access behaviour using the server logs. The scheme offers traffic intensity and web content independent defence approach against proxy based attacks. However with the increase in number of users, the model is likely to give expensive results. Liao et al. (2015) proposed a detection scheme based on support vector machine. The detection is based on similarity of bots in accessing the web pages. They used feature like request frequency sequence to record the request patterns of users and apply rhythm matching algorithm to identify similar patterns. The similarity based detection can be evaded by new and stealthy bots. Xiao et al. (2015) proposed a detection scheme based on the property that the flows generated by the same software are likely to be correlated with each other. They used k-nearest neighbours algorithm to identify the flows that may have occurred from the same software or bots. However, if an attacker uses different configuration parameters for initiating an attack from the bots then bots may generate non-similar flows.

DDoS attacks are usually executed using a set of geographically separated compromised machines (bots), controlled by a bot-master whereas FE originates from a large number of legitimate clients trying to access a web-resource simultaneously. Therefore, this problem of differentiating DDoS attacks from FEs can be mapped onto the problem of ensuring that a human user (rather than DDoS agent software) is at the other end of a network connection, typically by performing the so-called reverse Turing tests. The most commonly used type of reverse Turing test displays a slightly blurred or distorted picture or some puzzle and asks the user to type in the depicted symbols (Von Ahn et al., 2004). This task is easy for humans, yet very