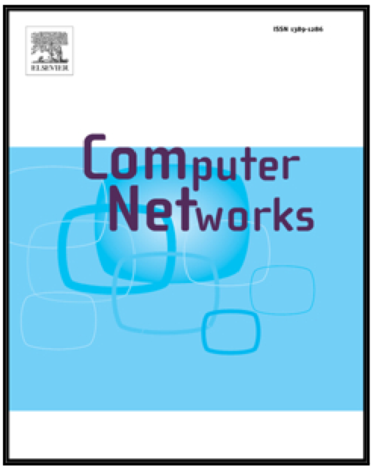
Accepted Manuscript



Detection of DDoS Attacks and Flash Events using Novel Information Theory Metrics

Sunny Behal, Krishan Kumar

PII: S1389-1286(17)30059-2
DOI: 10.1016/j.comnet.2017.02.015
Reference: COMPNW 6114

To appear in: *Computer Networks*

Received date: 29 August 2016
Revised date: 23 January 2017
Accepted date: 21 February 2017

Please cite this article as: Sunny Behal, Krishan Kumar, Detection of DDoS Attacks and Flash Events using Novel Information Theory Metrics, *Computer Networks* (2017), doi: 10.1016/j.comnet.2017.02.015

Detection of DDoS Attacks and Flash Events using Novel Information Theory Metrics

Sunny Behal, Krishan Kumar

Research Scholar, IKG Punjab Technical University, Punjab, India
Department of Computer Science and Engineering, SBS State Technical Campus, Punjab, India,
Corresponding Author: Sunny Behal, Email: sunnybehal@sbsstc.ac.in

***Abstract*—Distributed Denial of Service (DDoS) is an austere menace to network security. The in-time detection of DDoS attacks poses a stiff challenge to network security professionals. In this paper, the authors initiatively propose using a novel set of information theory metrics called ϕ-Entropy and ϕ-Divergence metrics for detecting DDoS attacks and flash events. The proposed metrics are highly sensitive towards detecting meek variations in the network traffic and elicit more information distance between legitimate and attack traffic flows as compared to existing predominantly used Generalized Entropy (GE) and Generalized Information Divergence (GID) metrics. As part of this work, a generalized detection algorithm has been proposed which uses the entropy difference between traffic flows to detect different types of DDoS attacks and FEs. The proposed detection algorithm has been validated using various publically available datasets of MIT Lincoln, CAIDA, FIFA and synthetically generated DDoSTB dataset in terms of various detection system evaluation parameters.**

***Index Terms*—DDoS Attacks, Network Security, Entropy, Information Divergence.**

I. Introduction

DDoS attacks pose a very critical threat to network security in general. DDoS attacks are in existence for many years. In a DDoS attack, the legitimate users are deprived of using web-based services. Typically, a DDoS attack is launched in a coordinated manner by compromising millions of computer systems available freely on the Internet [1]. The target service is denied by sending a redundant stream of packets to a victim rendering it unavailable to the legitimate clients. Usually, the prominent websites are the prime victims of such attacks. Recently Twitter, Spotify, and Amazon suffer interruptions in their services for almost two hours on Oct 21, 2016, because of DDoS attacks. Such interruptions in the services lead to massive financial losses. The revenue loss has amplified to \$209 million in the first quarter of 2016, as compared to \$24 million for all of 2015 [2]. As per worldwide infrastructure security report (WISR) [3], high-rate DDoS attacks (HR-DDoS) are predominant nowadays, having traffic volume more than 600 Gbps. It is crucial to detect such attacks in time to ensure the timely delivery of the widely used Internet-based services and applications. However, it is comparatively easy to detect HR-DDoS attacks, as their traffic profile deviates significantly from the normal traffic profile of the network. As per Wang et al. [4], the sophisticated attackers are shifting their focus in carrying out more subtle and stealthy low rate DDoS (LR-DDoS) attacks. Such LR-DDoS attacks are comparatively harder to detect because of the similarity of traffic rate and other traffic features with that of legitimate traffic, and hence can easily evade the traditional anomaly-based detection systems.

Recently, there is an another kind of network traffic apart from HR-DDoS and LR-DDoS attacks, which is gaining popularity among the security researchers, and which also causes a denial of service to legitimate users of a web service, called a flash event (FE). An FE is similar to an HR-DDoS attack wherein thousands of legitimate users try to access a particular computing resource such as a website simultaneously [5]. This sudden surge in legitimate traffic is mainly due to some breaking news happening around the world like the publishing of Olympic schedule or new product launch by top notch companies like Apple, Samsung, etc. It causes the untimely delivery of responses from a web service and thus, requires immediate action. A recent flash event occurred against the Australian census website on August 21, 2016. Millions of users simultaneously access the census website to fill their personnel details. The lack of sufficient resources on the web server causes the website to crash down. It is interesting to note that the Arbor Networks say it wasn't a DDoS attack, but more likely an FE whereas the officials pretend it to be a series of DDoS attacks [6]. Such situations highlight the severity of the problem.

Both HR-DDoS attack and an FE share many common characteristics like a change in the rate of traffic volume, delay in responses from the webs server, etc. but still there are few parametric differences between them. The request rate per source IP is small in the case of an FE as in an HR-DDoS attack. Further, the similarity of network flows, less throughput and duration of traffic per source IP are some rationales that differentiate an HR-DDoS attack from an FE [5].

Recently, information theory-based detection metrics have been used progressively in network anomaly detection domain. The key attractions of using information theory-based metrics can be summarized as (a) they can easily characterize the different kinds of network traffic using few packet header features, (b) time and space complexity is small as only header information is used for calculation, (c) high scalability, (d) high sensitivity, and (e) low false positive rate [7]. For analyzing a sample in a time interval T with a total of n samples per time window, the information theory-based metrics takes