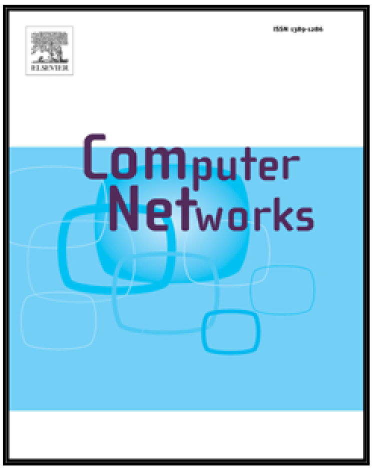
Accepted Manuscript



Woodpecker: Detecting and Mitigating Link-flooding Attacks via SDN

Lei Wang, Qing Li, Yong Jiang, Xuya Jia, Jianping Wu

PII: S1389-1286(18)30972-1
DOI: https://doi.org/10.1016/j.comnet.2018.09.021
Reference: COMPNW 6603

To appear in: *Computer Networks*

Received date: 15 February 2018
Revised date: 23 August 2018
Accepted date: 26 September 2018

Please cite this article as: Lei Wang, Qing Li, Yong Jiang, Xuya Jia, Jianping Wu, Woodpecker: Detecting and Mitigating Link-flooding Attacks via SDN, *Computer Networks* (2018), doi: https://doi.org/10.1016/j.comnet.2018.09.021

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Woodpecker: Detecting and Mitigating Link-flooding Attacks via SDN

Lei Wang[a], Qing Li[b,*], Yong Jiang[a], Xuya Jia[a], Jianping Wu[c]

[a]*Graduate School at Shenzhen, Tsinghua University, Shenzhen, China*
[b]*Southern University of Science and Technology, Shenzhen, China*
[c]*Department of Computer Science and Technology, Tsinghua University, Beijing, China*

Abstract

Link-flooding attack (LFA), as a new type of DDoS attack, can degrade or even cut off network connectivity of a target area. This attack employs legitimate, low-density flows to flood a group of selected links. Therefore, these malicious flows can hardly be distinguished by traditional defense technologies. In our scheme, we first select M routers and upgrade them into SDN switches to maximize the network connectivity. Then, we propose a proactive probe approach to rapidly locate the congested links. Next, our scheme employs a global judgment algorithm to determine whether the network is under LFA or not. Finally, Woodpecker employs the core defense measure that based on the centralized traffic engineering to make the traffic balanced and eliminate the routing bottlenecks that are likely to be utilized by the adversary. We evaluate our scheme through comprehensive experiments. The results show that the bandwidth utilization of LFA-attacked links can be reduced by around 50% and that the average packet loss rate and jitter can be effectively decreased under LFA attacks.

Keywords: `Link-flooding Attack, DDoS, Software-Defined Networking`

ACCEPTED MANUSCRIPT

1. Introduction

Recently, distributed denial of service (DDoS) attacks are the biggest threat to the availability of networks, applications and cloud services. The adversary generally explores resource asymmetry between the bots and victim servers, and abuses vulnerabilities of many network protocols to launch DDoS attacks [1, 2]. Many effective approaches have been proposed to detect and defend against the DDoS attacks, including Pushback [3], Ingress filter [4], PacketScore [5] and so forth. These methods all need to identify malicious traffic in advance, but this operation is very difficult for link-flooding attack (LFA) — a new type of DDoS attack.

Different from the traditional DDoS attacks, LFA floods a well-chosen group of links to cut off the network connections of a target area, instead of attacking the target servers directly. To this end, the adversary first detects the paths from bots to the public servers and constructs a link map accordingly. Then, the adversary floods the selected links by employing a large number of bots to send legitimate, low-density flows to the certain public servers. In this way, these congested links will severely degrade or even cut off the network connections of the target area. We show a simple example of LFA in Figure 1.

Over the last few years, LFA has quickly moved from the realm of academic curiosity [6, 7] to real-world incidents. We have already witnessed the real-life demonstration of LFA in the core of the Internet [8, 9]. The target areas of these attacks include internet exchange points, enterprises and campus. Worth still, such an attack may be more frequent and massive due to inability to resist in reality.

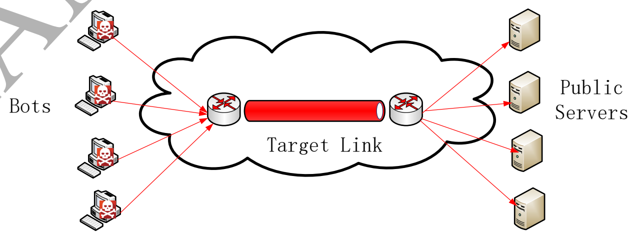


Figure 1: An Example of Link-flooding Attack

LFA typically has two remarkable characteristics. **Undetectablity:** The target area is not directly attacked. Thus the servers in the target area cannot perceive any suspicious traffic. **Indistinguishability:** The adversary usually employs legitimate, low-rate flows with real IP addresses. Consequently, it is difficult to distinguish malicious flows from legitimate ones.

Because of the above characteristics, the traditional countermeasures, such as local rerouting and flow filtering based on traffic-intensity, have little effect on mitigating LFA. Moreover, LFA can change the selected links or the bot-server pairs periodically. Take a typical LFA — the Crossfire attack [6] as an example. Such attack alternately floods the optimal group of links for 3 minutes and another non-intersecting sub-optimal group of links for 30 seconds.

In summary, there are three significant challenges to de-

[*] Corresponding author
Email address: `liq8@sustc.edu.cn` (Qing Li)

Download English Version:

https://daneshyari.com/en/article/11009327

Download Persian Version:

https://daneshyari.com/article/11009327

Daneshyari.com