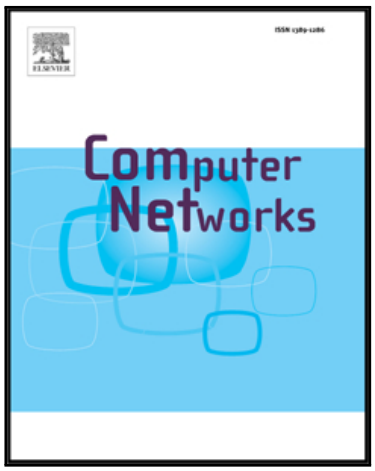
Accepted Manuscript



Power Spectrum Entropy based Detection and Mitigation of Low-Rate DoS Attacks

Zhaomin Chen, Chai Kiat Yeo, Bu Sung Lee, Chiew Tong Lau

PII: S1389-1286(18)30102-6
DOI: 10.1016/j.comnet.2018.02.029
Reference: COMPNW 6427

To appear in: *Computer Networks*

Received date: 20 May 2017
Revised date: 18 January 2018
Accepted date: 28 February 2018

Please cite this article as: Zhaomin Chen, Chai Kiat Yeo, Bu Sung Lee, Chiew Tong Lau, Power Spectrum Entropy based Detection and Mitigation of Low-Rate DoS Attacks, *Computer Networks* (2018), doi: 10.1016/j.comnet.2018.02.029

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

Power Spectrum Entropy based Detection and Mitigation of Low-Rate DoS Attacks

Zhaomin Chen, Chai Kiat Yeo, Bu Sung Lee, Chiew Tong Lau

Computer Network and Communication Graduate Lab
School of Computer Science and Engineering
Nanyang Technological University, Singapore 639798

Abstract

Low-Rate DoS (LDoS) attacks send periodical packet bursts to the bottleneck routers which can throttle the bandwidth of TCP flows. They are difficult to detect while severely degrading the Quality of Service (QoS) of TCP applications. By combining Power Spectrum Analysis with Information Entropy, we introduce two novel information metrics to detect the LDoS attacks: Fourier Power Spectrum Entropy (FPSE) and Wavelet Power Spectrum Entropy (WPSE). As the energy of LDoS attack signal is mostly concentrated in the low-frequency range, FPSE and WPSE of LDoS attacks both exhibit lower values compared to those of normal flows. Therefore, these two metrics can be applied here to detect LDoS attacks efficiently. By evaluating on NS-3 simulations and real network traces, the results validate the effectiveness of these two metrics to differentiate LDoS attacks from normal flows. They can detect the LDoS attacks efficiently with fewer false alarms compared to the other detection mechanisms. Based on these two metrics, we also propose a Power Spectrum Entropy-based Robust-RED (PRRED) queuing algorithm to mitigate LDoS attacks. The evaluation results in NS-3 demonstrate that the proposed algorithm is able to effectively preserve the TCP bandwidth while countering the different LDoS attacks.

Keywords: Low-Rate DoS (LDoS) Attacks, Power Spectrum Entropy (PSE), Fourier Power Spectrum Entropy (FPSE), Wavelet Power Spectrum Entropy

Email address: {chen0954, asckyeo, ebslee, asctlau}@ntu.edu.sg (Zhaomin Chen, Chai Kiat Yeo, Bu Sung Lee, Chiew Tong Lau)

ACCEPTED MANUSCRIPT

Download English Version:

https://daneshyari.com/en/article/6882706

Download Persian Version:

https://daneshyari.com/article/6882706

Daneshyari.com