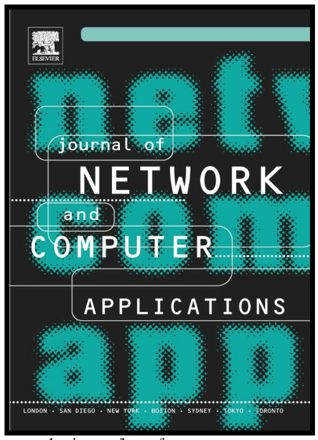
Author's Accepted Manuscript

Stealthy Denial of Service (DoS) Attack Modelling and Detection for HTTP/2 Services

Erwin Adi, Zubair Baig, Philip Hingston



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30163-7
DOI: http://dx.doi.org/10.1016/j.jnca.2017.04.015
Reference: YJNCA1912

To appear in: *Journal of Network and Computer Applications*

Received date: 7 December 2016
Revised date: 3 April 2017
Accepted date: 26 April 2017

Cite this article as: Erwin Adi, Zubair Baig and Philip Hingston, Stealthy Denia of Service (DoS) Attack Modelling and Detection for HTTP/2 Services, *Journa of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2017.04.015

Stealthy Denial of Service (DoS) Attack Modelling and Detection for HTTP/2 Services

Erwin Adi, Zubair Baig, Philip Hingston*

School of Science

Edith Cowan University

270 Joondalup Drive, Joondalup WA 6027, Australia

Abstract

A malicious attack that can prevent establishment of Internet connections to web servers is termed as a Denial of Service (DoS) attack; volume and intensity of which is rapidly growing thanks to the readily available attack tools and the ever-increasing network bandwidths. Contemporary web servers are increasingly vulnerable to such attacks. With the emergence of HTTP/2 as the successor of HTTP/1.x, existing techniques for detecting DoS attacks will not be entirely effective. Though nearly 90% of all contemporary web servers as yet have not migrated to HTTP/2, DoS attack modelling and detection is essential to prevent impending attacks of such kind from the adversary class. This study presents a model of DoS attack traffic that can be directed towards HTTP/2 web servers. The research conducted also extends previous studies that provided DoS attack models against HTTP/2 services, to present a novel and stealthy DoS attack variant that can disrupt routine web services, covertly. The attack traffic analysis conducted in this study employed four machine learning techniques, namely Naïve Bayes, Decision Tree, JRip and Support Vector Machines, and stealthy traffic properties are shown through having higher percentages of False Alarms. Results obtained through simulation show promise, and arguments are put forth on how future work can extend the proposed model to create further

*Corresponding author

Email addresses: `z.baig@ecu.edu.au` (Erwin Adi, Zubair Baig, Philip Hingston)