Filtration Model for the Detection Of Malicious Traffic In Large-Scale Networks

Abdulghani Ali Ahmed[a] ,Aman Jantan[b,] , Tat-Chee Wan[b]

[a] Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Pahang, Malaysia

[b] School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia

ABSTRACT

This study proposes a capable, scalable, and reliable edge-to-edge model for filtering malicious traffic through real-time monitoring of the impact of user behavior on quality of service (QoS) regulations. The model investigates user traffic, including that injected through distributed gateways and that destined to gateways that are experiencing actual attacks. Misbehaving traffic filtration is triggered only when the network is congested, at which point burst gateways generate an explicit congestion notification (ECN) to misbehaving users. To investigate the behavior of misbehaving user traffic, packet delay variation (PDV) ratios are actively estimated and packet transfer rates are passively measured at a unit time. Users who exceed the PDV bit rates specified in their service level agreements (SLAs) are filtered as suspicious users. In addition, suspicious users who exceed the SLA bandwidth bit rates are filtered as network intruders. Simulation results demonstrate that the proposed model efficiently filters network traffic and precisely detects malicious traffic.

KEYWORDS: ECN; Malicious traffic; QoS regulations; SLA guarantees; User violations

DOI: 0.1016/j.comcom.2015.10.012