Computer Communications 82 (2016) 59–70

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Filtration model for the detection of malicious traffic in large-scale networks

Abdulghani Ali Ahmed [a,*], Aman Jantan [b,1], Tat-Chee Wan [b,2]

[a] Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Pahang, Malaysia
[b] School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia

ARTICLE INFO

Article history:
Received 4 February 2015
Revised 14 October 2015
Accepted 31 October 2015
Available online 10 November 2015

Keywords:
ECN
Malicious traffic
QoS regulations
SLA guarantees
User violations

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.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Network intruders continuously formulate new sophisticated tactics of network intrusion. Generating an immense volume of unsolicited malicious traffic is one of their tactics for overwhelming network resources and disrupting online services for users. A sudden surge in network traffic mostly occurs because of malicious traffic generated from single or distributed sources to prevent legitimate users from using network resources or online services. Malicious traffic may cause failure in conducting e-businesses, accessing network information, or running online services [1].

Typically, malicious traffic can be generated through several technical strategies, such as botnet [2,3], distributed denial of service (DDoS) [4], and Slashdot effect [5]. According to J. Jaeyeon, K. Balachander, and R. Michael [6], the Slashdot effect attack damages the visited site similar to the DDoS attack, although the former may not always be an attack or a malicious distribution. The abovementioned strategies create huge traffic to execute an attack. Thus, development of an effective system to filter malicious packets is valuable for all botnet, DDoS, and Slashdot effect attacks.

The success of malicious traffic filtration methods depends on accuracy, scalability, and reliability. The accuracy of these methods is challenged when malicious and legitimate traffics are similar [7]. The scalability challenge arises because filtering malicious traffic at the early stage requires extra overhead in a volume, which mostly results in performance degradation [8]. The reliability of these methods is challenged when user traffic cannot be investigated in whole or in part. Such a case can be caused by a single point of failure when making filtration decisions.

Recent studies [7–15] have proposed methods to filter malicious packets and verify intruder attempts by monitoring the impact of user behavior on the service level agreement (SLA). According to [16], SLA is an electronic contract between the service provider and its users, a contract that defines the thresholds of quality of service (QoS) metrics that the provider commits to provide the user. The service provider uses random early detection (RED) to prevent congestion at its gateway queues by policing user traffic, which may exceed the predefined bit rate in the SLA [17]. As described in [18], RED is an active queue management mechanism that performs traffic policing depending on the gateway's average queue size, which is calculated for every packet arriving at the gateway queue.

To prevent incipient traffic burst, the RED gateway notifies the user of congestion to reduce its window size once the average queue size (AQS) exceeds a predefined threshold. A bursting gateway notifies the user of congestion in a probability approximately commensurate with the bandwidth share of that user [17]. According to [19,20], notifications of RED gateways for misbehaving users can be either

* Corresponding author. Tel.: +60 9 5492110; fax: +60 9 5492144.
E-mail addresses: abdulghani@ump.edu.my (A.A. Ahmed), aman@cs.usm.my (A. Jantan), tcwan@cs.usm.my (T.-C. Wan).
[1] Tel.: +60 4 653 4642; fax: +60 4 6573335.
[2] Tel.:+60 4 653 4633, +60 4 653 3617; fax: +60 4 6573335.

http://dx.doi.org/10.1016/j.comcom.2015.10.012
0140-3664/© 2015 Elsevier B.V. All rights reserved.

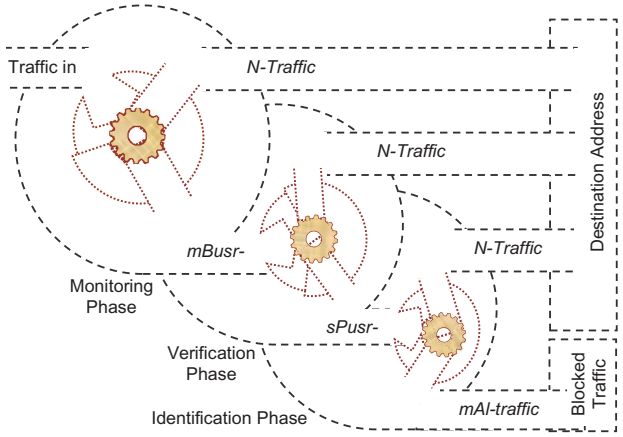

Fig. 1. Phases of traffic filtration.

implicit (dropping packets at gateway queues) or explicit (marking a bit in packet headers). According to [21–23], explicit notification is employed by modifying RED gateways to set a mechanism of TCP explicit congestion notification (ECN) in the header of IP packets. RED can deny a user from sending more bit rates than those specified in the SLA through a single gateway. However, it cannot deny the violation if the user sends it through multiple ingresses at a rate lower than the SLA bit rate.

The current paper proposes a distributed edge-to-edge model to detect and filter malicious traffic generated through several gateways and to delimit responsible users through three principal phases: monitoring, detection, and identification (Fig. 1). In the monitoring phase, ECN is primarily exploited to trigger traffic filtration. During traffic congestion, RED gateways distributed on the domain ingress edges are used to uncover a user with ECN as a misbehaving user (*mBusr*) and to classify its traffic as misbehaving user traffic (*mBusr-traffic*). In the detection phase, an *mBusr* with packet delay variation (PDV) ratios exceeding the predefined ratios in the SLA is classified as a suspicious user (*sPusr*), and its traffic is filtered as suspicious user traffic (*sPusr-traffic*). In the identification phase, an *sPusr* that exceeds the packet transmission rate (PTR) ratios guaranteed in the SLA is a malicious user, and its injected traffic is malicious traffic (*mAl-traffic*). Users who do not violate the ratios specified in the SLA are classified as legitimate users, and their traffic is filtered as normal traffic (*N-traffic*).

The novelty of this study is represented through several potential contributions. First, this study develops a scalable method for monitoring user violations of QoS regulations. The method benefits from ECNs, which are issued by RED gateways to misbehaving end users. ECNs inform misbehaving end users about the need to reduce the window size of data transmission. Thus, monitoring of user traffic is triggered only when burst gateways actually generate an ECN to *mBusrs*. Second, this study presents a reliable load-balancing technique for reducing the overhead required to make decisions on traffic filtration. This technique is deployed using multi-management units that are interconnected on the basis of a virtual overlay network. The virtual structure of overlay networks is exploited to exchange filtration messages among the management units and to finalize decisions on traffic filtration. This technique also benefits from the anycast protocol for supporting one-to-one transmission among the gateway routers and the nearest overlay network management unit. Third, this study proposes a new solution to the problem of single-point failure in the decision maker agent. This solution involves multi-management units connected through a virtual overlay network. When a particular unit fails, the overlay network maintains its structure and sets the nearest unit for the ingress edges closest to the unit of failure. Lastly, this study defines a deficiency method for improving the accuracy of traffic filtration and for distinguishing *mAl-traffic* from *N-Traffic*. The accuracy of this method depends on the passive measurement of transmission rates, although only for the *sPusr* filtered in the previous stage of ECN monitoring.

The rest of the paper is organized as follows. Section 2 discusses related works. Section 3 describes the architecture of malicious traffic filtration. Section 4 presents the deployment of agents. Section 5 describes the malicious traffic filtration policy. Section 6 presents the experimental results and analytical evaluation. Finally, Section 7 concludes and discusses the possibilities for future work.

2. Related work and comparison

Many real-time studies have investigated the impact of user behavior on QoS regulations to filter malicious traffic. Anomaly behavior is detected when its impact on QoS regulations exceeds a particular threshold. The threshold values, which distinguish normal from abnormal impact, are defined either by specifying a predefined ratio or by the threshold ratio obtained through training the system on a normal pattern. The following subsections classify the related work of this paper based on the way of specifying the thresholds and critically analyze their existing limitations.

2.1. Classification of threshold-based approaches

In this paper, related works are classified into three directions depending on how they specify threshold values: learned, adaptive, and predefined threshold-based approaches. Learned threshold-based approaches have been studied in the past [24–27]. Trained thresholds are created by learning network traffic patterns on a particular network for a specific period (e.g., days, weeks, or months). According to [23], the threshold is trained with traces of normal system behavior. Observed event streams are then fed into the trained threshold, which classifies these streams as normal (the observations match the training data) or anomalous. Adaptive threshold-based approaches have been studied in the past [17,18,28]. Adaptive threshold is a varying threshold whose value is calculated automatically. The value of this threshold is set dynamically and adaptively on the basis of a particular estimation computed from recent traffic measurements. According to [17], the adaptive threshold algorithm is a simple algorithm that detects anomalies on the basis of violations of a threshold that is adaptively set following recent traffic measurements. One advantage of using the adaptive threshold is that it improves accuracy and reduces human intervention by accurately tracking varying real-time measurements [17].

Predefined threshold-based approaches refer to preset values considered as a baseline to separate two different behaviors (i.e., normal or abnormal). This baseline method compares the observed behavior with lower and higher bounds of the threshold. Whenever the behavior goes below the lower bound threshold or above the higher bound threshold, a violation to the thresholds is detected, and the baseline method raises an alarm. The predefined thresholds are commonly used in statistical-based detection mechanisms. Table 1 describes the general limitations of the threshold-based approaches.

2.2. Critical analysis

The proposed study avoids the aforementioned limitations of learned-based approaches by using a hybrid of adaptive and predefined thresholds that are not required in the learning process for malicious traffic detection. The adaptive threshold is used in the phase of network traffic monitoring by utilizing RED thresholds. The predefined threshold is used in the following stages of malicious traffic filtration by utilizing SLA thresholds. Therefore, the aforementioned limitations of adaptive threshold are avoided by using predefined

Download English Version:

https://daneshyari.com/en/article/449926

Download Persian Version:

https://daneshyari.com/article/449926

Daneshyari.com