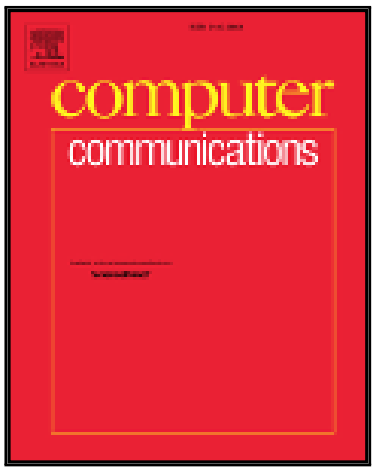
Accepted Manuscript



Distributing Data Analytics for Efficient Multiple Traffic Anomalies Detection

Alba P. Vela , Marc Ruiz , Luis Velasco

PII: S0140-3664(16)30321-8
DOI: 10.1016/j.comcom.2017.03.008
Reference: COMCOM 5481

To appear in: *Computer Communications*

Received date: 12 September 2016
Revised date: 21 December 2016
Accepted date: 21 March 2017

Please cite this article as: Alba P. Vela , Marc Ruiz , Luis Velasco , Distributing Data Analytics for Efficient Multiple Traffic Anomalies Detection, *Computer Communications* (2017), doi: 10.1016/j.comcom.2017.03.008

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

Distributing Data Analytics for Efficient Multiple Traffic Anomalies Detection

Alba P. Vela*, Marc Ruiz, and Luis Velasco

Universitat Politècnica de Catalunya (UPC), Barcelona, Spain.
*Corresponding author: apvela@ac.upc.edu

***Abstract*—Traffic anomalies can create network congestion, so its prompt and accurate detection would allow network operators to make decisions to guarantee the network performance avoiding services to experience any perturbation. In this paper, we focus on origin–destination (OD) traffic anomalies; to efficiently detect those, we study two different anomaly detection methods based on data analytics and combine them with three monitoring strategies. In view of the short monitoring period needed to reduce anomaly detection, which entails large amount of monitoring data to be collected and analyzed in a centralized repository, we propose bringing data analytics to the network nodes to efficiently detect traffic anomalies, while keeping traffic estimation centralized. Once an OD traffic anomaly is detected, a network reconfiguration can be triggered to adapt the network to the new traffic conditions. However, an external event might cause multiple related traffic anomalies. In the case of triggering a network reconfiguration just after one traffic anomaly is detected, some Key Performance Indicators (KPI) such as the number of network reconfigurations and the total reconfiguration time would be unnecessarily high. In light of that, we propose the Anomaly and Network Reconfiguration (ALCOR) method to anticipate whether other ODs are anomalous after detecting one anomalous OD pair. Exhaustive simulation results on a realistic network scenario show that the monitoring period should be as low as possible (e,g., 1 min) to keep anomaly detection times low, which clearly motivates to place traffic anomaly detection function in the network nodes. In the case of multiple anomalies, results show that ALCOR can significantly improve KPIs such as the number of network reconfigurations, total reconfiguration time, as well as traffic losses.**

***Keywords*—Traffic anomalies; data analytics placement; network reconfiguration**

I. OD TRAFFIC ANOMALIES

Traffic anomalies are short-living events that do not follow expected patterns (see a survey in [1]). They can create network congestion and stress resource utilization in packet nodes and hence, its prompt detection becomes essential since it allows preparing the network e.g., by reconfiguring the virtual network topology in multilayer network scenarios [2]. Anomaly detection can be used to trigger lightpath provisioning and network re-configuration when a traffic anomaly is detected [3], which entails analyzing monitoring data to anticipate traffic congestion. It is clear that developing efficient techniques to detect traffic anomalies in real time would empower network operators to prevent grave consequences induced by such anomalies affecting end users. However, detecting anomalies is a difficult task because anomalous patterns need to be extracted and interpreted from large amounts of high-dimensional, noisy data.

In order to detect traffic anomalies, it is essential to monitor traffic at the nodes and to model such traffic [4]. For packet networks specifically, the traffic monitoring function allows identifying (classifying) the traffic belonging to a specific service or destination, so as to apply specific policies. Monitoring traffic samples are produced at the packet nodes; according to the ITU-T [5], performance events are counted second by second over every 15-minute period. At the end of a period, they are collected in a repository for further analysis [2], [6]; for instance, data analysis can be used to create predicted traffic matrices for the near future; please refer to [7] for a list of use cases of traffic monitoring. Among use cases, that of identifying network failures [8], [9] and problems (or anomalies) is undoubtedly of the interest of many network operators. It is clear that when analytics are applied to data collected every 15 minutes, the expected traffic anomaly detection times will be as well in that order of magnitude. Consequently, the monitoring period should be reduced, which in turn increases the amount of monitoring data to be sent to the centralized data repository.

Many works in the literature can be found focused on intrusion and denial-of-service (DoS) detection (see e.g., [10]). Regarding traffic anomalies, authors in [11] proposed a general method that entails monitoring traffic in links and correlate monitoring time series to detect volume anomalies, identify the origin-destination (OD) pair, and estimate the amount of traffic involved in the anomalous OD pair. The method is based on applying Principal Component Analysis (PCA) to separate the multidimensional space occupied by a set of network traffic samples into

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات