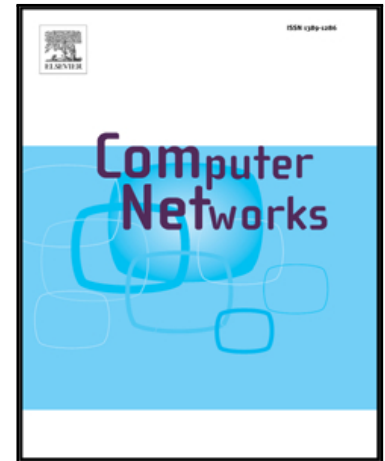


Accepted Manuscript

Measurement of Large-scale BGP Events: Definition, Detection, and Analysis

Meng Chen, Mingwei Xu, Qing Li, Yuan Yang

PII: S1389-1286(16)30315-2
DOI: [10.1016/j.comnet.2016.09.018](https://doi.org/10.1016/j.comnet.2016.09.018)
Reference: COMPNW 6017



To appear in: *Computer Networks*

Received date: 18 May 2016
Revised date: 18 August 2016
Accepted date: 20 September 2016

Please cite this article as: Meng Chen, Mingwei Xu, Qing Li, Yuan Yang, Measurement of Large-scale BGP Events: Definition, Detection, and Analysis, *Computer Networks* (2016), doi: [10.1016/j.comnet.2016.09.018](https://doi.org/10.1016/j.comnet.2016.09.018)

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.

Measurement of Large-scale BGP Events: Definition, Detection, and Analysis

Meng Chen^a, Mingwei Xu^a, Qing Li^b, Yuan Yang^a

^a*Dept. of Computer Science and Technology, Tsinghua University, China*

^b*Graduate School at Shenzhen, Tsinghua University, China*

Abstract

Measurement on the Border Gateway Protocol (BGP) system is important for understanding the Internet. Many attempts have been made to detect anomalous Internet events through dissecting BGP updates and tables. We notice that most works in this field either deploy/use few monitors or analyze aggregated statistics. Such practices may result in overestimating the impact of monitor-local events, which can be viewed by only a small area.

We propose Large-scale BGP Event (LBE), which affects many IP prefixes (high impact) and is widely observable (non-local). To detect LBE, we propose the Update Visibility Matrix (UVM) to record the prefix and monitor related to each update. We formulate the problem of identifying LBE in UVM, which is NP-hard. Then we propose a heuristic algorithm to solve it. We apply the scheme to 2.18 TB of BGP updates and find that the identified LBEs are highly correlated with many well-known disruptive incidents. Besides, we identify 101 LBEs that have never been investigated before. By conducting case studies, we find that the LBEs have high impact and are caused by various reasons. Our work can assist in network/Internet management tasks such as problem prevention, diagnosis, and recovery.

Key words: BGP, measurement, anomaly detection

1. Introduction

Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol. It is a path vector protocol, enabling the exchange of routing and reachability information among tens of thousands of Autonomous Systems (ASs, one or more networks under the control of a single administrative entity) on the Internet. The stability and robustness of the BGP system is always an important topic. With decades of effort, the BGP system is robust under most circumstances. However, big disruptive events can still seriously affect the connectivity

*Corresponding Author: Meng Chen; East Main Building 9-325, Tsinghua University, Beijing, China; chenm11@mails.tsinghua.edu.cn; (+86) 13581986149

Download English Version:

<https://daneshyari.com/en/article/4954868>

Download Persian Version:

<https://daneshyari.com/article/4954868>

[Daneshyari.com](https://daneshyari.com)