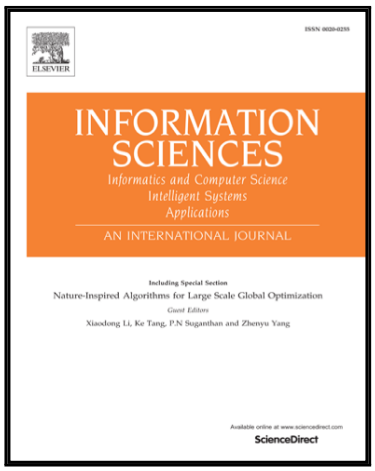

Efficient Alarm Behavior Analytics for Telecom Networks

Jiantao Wang, Caifeng He, Yijun Liu, Guangjian Tian, Ivy Peng, Jia Xing, Xiangbing Ruan, Haoran Xie, Fu Lee Wang

PII: S0020-0255(17)30605-9
DOI: 10.1016/j.ins.2017.03.020
Reference: INS 12803

To appear in: *Information Sciences*

Received date: 25 July 2016
Revised date: 17 March 2017
Accepted date: 18 March 2017

Please cite this article as: Jiantao Wang, Caifeng He, Yijun Liu, Guangjian Tian, Ivy Peng, Jia Xing, Xiangbing Ruan, Haoran Xie, Fu Lee Wang, Efficient Alarm Behavior Analytics for Telecom Networks, *Information Sciences* (2017), doi: 10.1016/j.ins.2017.03.020

Efficient Alarm Behavior Analytics for Telecom Networks

Jiantao Wang[a], Caifeng He[a], Yijun Liu[a], Guangjian Tian[a], Ivy Peng[a],
Jia Xing[a], Xiangbing Ruan[a], Haoran Xie[b,*], Fu Lee Wang[c]

[a]*Noah's Ark Lab, Huawei Technologies, Hong Kong SAR, China*
[b]*Department of Mathematics and Information Technology,*
The Education University of Hong Kong, Hong Kong SAR, China
[c]*Caritas Institute of Higher Education, Hong Kong SAR, China*

Abstract

Locating network fault problems and filtering trivial alarms from important ones are the two main challenges in Network Operation Centers (NOCs). In this paper, we present an alarm behavior analysis and discovery system, AABD, that establishes flapping and parent-child (P-C) rules to reveal the operation patterns from a large number of alarms in telecom networks. These rules can be exploited to filter out unimportant alarms, conduct multi-dimensional analysis of the alarms and identify potential network problems. We propose two novel and effective algorithms to establish the flapping rules and P-C rules. The proposed system is validated using alarm datasets from five Internet service providers. Specifically, we verify the system and methodology in each of the five network domains, i.e., circuit-switched network (CS), packet-switched network (PS), 2G-radio access network (RAN-2G), 3G-radio access network (RAN-3G) and 4G-radio access network (RAN-4G), as these five domains can, to a great extent, form a complete network environment. More importantly, our system can establish a small number of rules, only dozens of flapping rules and P-C rules, and compress the alarms by approximately 84%, i.e., 84% of alarms will not be sent to the network operator. To summarize, the proposed system can help network operators respond to network faults in a timely fashion, locate the faults accurately and significantly reduce the time spent on these tasks.

Keywords: Alarm Analysis and Discovery, Correlation, Telecom, Big Data, Data Mining, Frequent Pattern Mining

1. Introduction

In recent years, we have witnessed the rapid growth of telecom (telecommunication) networks in both scale and topological complexity with the increasing deployment of 4G-cellular, e.g., LTE equipment. However, the management of such complex and large networks has become a challenging issue. Network operators are compelled to monitor and process alarms to provide high-quality service to their customers. For a network service provider, the quality of services offered and the efficiency of identifying/fixing faults in telecom networks are the key criteria to become more competitive than other network providers, avoid/reduce churn and attract new customers.

An important way to sustain high-quality services is to address network faults in a timely manner. Every day, tens of thousands of faults are triggered across heterogeneous and interconnected devices in a telecom network. These faults are expressed by the network devices in the form of alarms, which are transmitted to the Network Operation Centre (NOC) for further processing by network operators. Additionally, there are thousands of types of alarms. If the network operators handle all alarms sequentially, they will be overloaded and unable to concentrate on finding the underlying reasons for the faults. Generally, approximately 1 million alarms are reported to the NOC every day. If there are five network operators working 8 hours per day, each operator must process 20 alarms every minute throughout the day, which is an impossible workload. Therefore, it is necessary to select the important alarms that are useful for identifying network problems. There are two categories of approaches to filtering out trivial alarms. First, some types of alarms occur with high frequency but only last for a few hundred seconds or even shorter periods of time. Instead of receiving all alarms, the alarms that last for a long duration are sufficient for network operators to identify the underlying problems. Therefore, an approach to determining a proper rule by which the network operators can eliminate the trivial alarms is crucial. Second, alarms in different categories may be correlated with each other. For example, in the PS domain, if the alarm M3UA Signaling Link Failed occurs, alarm M3UA Route Unavailable will always occur within a few seconds. These correlations among alarms are called correlation rules, and they can be further exploited to 1) reduce the number of alarms sent to the network operators and 2) establish P-C (parent-child) rules to pinpoint the root causes of network faults. The network management system of the network provider normally focuses on processing alarms by identifying and compressing flapping alarms, identifying correlation alarms and locating the root cause of the alarms. Previous works [15, 23, 32, 2, 3] have investigated some aspects of these issues. In [15], a TASA system was proposed to determine the association and correlation rules rather than to address the flapping issues. In addition,

*Corresponding author. Tel.: +852 68502340
Email address: hrxie2@gmail.com (Haoran Xie)