Decision Support Systems 73 (2015) 57–73

Contents lists available at ScienceDirect

Decision Support Systems

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

Early detection of network element outages based on customer trouble calls

Željko Deljac [a,*], Mirko Randić [b], Gordan Krčelić [a]

[a] T-Hrvatski Telekom (T-HT), Technical Functions, Savska 32, Zagreb, Croatia
[b] Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

ARTICLE INFO

Article history:
Received 13 February 2014
Received in revised form 14 January 2015
Accepted 22 February 2015
Available online 3 March 2015

Keywords:
Fault management
Broadband network
Early fault detection
Alarm system
Fault detection delay

ABSTRACT

This paper deals with the issue of early detection of network element outages. Timeliness of outage detection as well as accuracy in finding outages on equipment in a telecommunication network depend on the monitoring system used and its performance. The intent of this paper is to investigate and propose a complementary solution to improve the performance of the existing systems in detecting faults earlier than it was able to do before. In developing our approach two constraints are given. The existing operational environment cannot be changed; threshold tuning and parameter changing cannot be done; furthermore no additional infrastructure investment has been planned. Hence, our approach relies on an alternative method based on a two-stage hybrid statistical and diagnostic detector which we designed in a way that exploits additional available data and avoids alarm monitoring system imperfections. The role of this detector is twofold: early detection of network element outages based on customer trouble calls and rule-based decision making for faulty-element isolation based on knowledge derived from fault and network management data. In this paper we present results of statistical analysis of trouble-reporting data. The analysis showed that the timing of customers' trouble reports and their content have information potential that can be utilized for early detection of outages. The detector is explained in detail and its accuracy and reduction delay is evaluated. The method presented can reduce the outage detection delay time by 2.33 h on average observed in relation to the performance of an existing fault management process which was designed to detect outages solely on the basis of an alarm monitoring system, for the "difficulties in work" type of malfunction. We attained an overall probability of correct detection of 95.3%. Out of the total number of outages that hypothetically could be detected, by using this method we were able to detect 77.5% of cases 1 h before the alarm was raised in the existing alarm system, while 23% of cases were detected 4 h before the actual alarm. The approach has been tested on real telecommunication network data over the period of one year.

1. Introduction

Broadband networks contain a multitude of hardware and software components in different locations that can be subject to fault. A typical broadband network (Fig. 1) consists of three main parts. The IP/MPLS core part (1) is based on Multiprotocol Label Switching (MPLS) technology. In addition, there are head-end servers that provide services to users such as: Internet access, access to video services, Internet Protocol TeleVision (IPTV), Video On Demand (VOD) and Voice Over Internet Protocol (VOIP) telephone services. In the access part of the network (2), Digital Subscriber Line Access Multiplexer (DSLAM) architecture is used to link customer traffic over an ADSL port to the Ethernet aggregation. The physical link between the subscriber and the DSLAM port is a twisted copper pair in subscriber cable — the most common kind of access. The end point of the access part is a Distribution point behind which the customer installation begins. The third part (3) includes network termination equipment (ADSL modem, Splitter), other CPEs (IPTV STB, TV, handset and other devices) and in-house customer installations. This part of the network is spatially most extensive.

From the perspective of broadband network management, faults can be categorized as those that affect services offered only to one particular customer and those that affect a whole group of customers. For example, a network element outage mostly degrades or disables services offered to a larger number of customers. As a result, more people start to report failures. After repair of this kind of fault, problems related to services of the whole group disappear. A fault management system is designed to record data related to all detected and resolved faults as well as reported failures. Most of the data refer to alarms that are used to detect and diagnose faults. Generally, all active network elements throw alarms, but there are passive pieces of equipment in the network incapable of producing alarms. Therefore, not all the network is under the real-time supervision of the fault management system. Data about alarms is entered into the database automatically while other data (e.g. about failures reported by customers) is entered by technicians during the resolving process. Accordingly, databases give an accurate

* Corresponding author. Tel.: +385 1 376 49 80.
E-mail address: zeljko.deljac@t.ht.hr (Ž. Deljac).

http://dx.doi.org/10.1016/j.dss.2015.02.014
0167-9236/

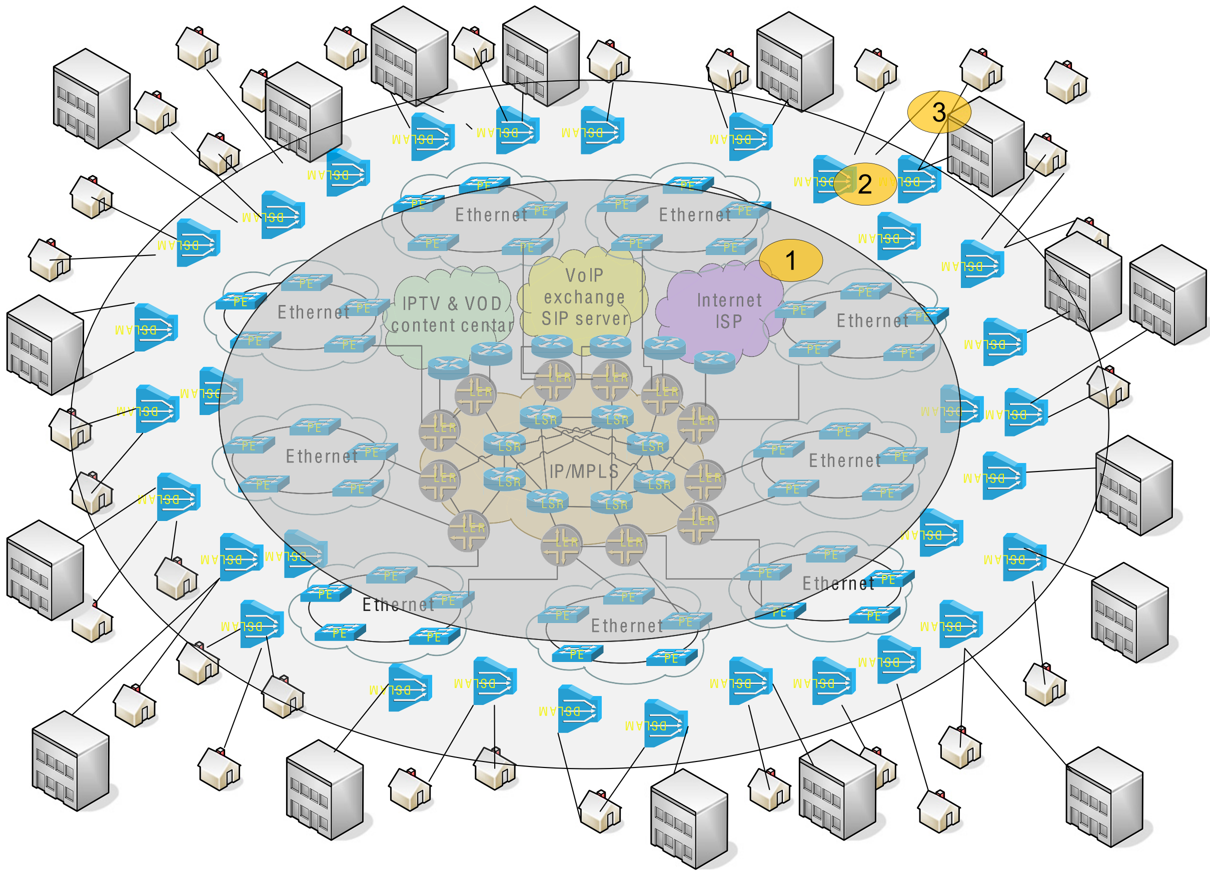

Fig. 1. Broadband network — main parts.
Source: T-HT (2012)

insight into faults, causes of faults and failures that have been reported. In [44] we presented results of the operational data analysis referring to the Croatian telecom T-HT broadband network. The following distribution of faults considering their locations has been derived from operational data. The majority, 70.86%, of faults occur in the customer part of the network (part 3). In the access part (part 2), 26.53% of faults appear, while the remainder, 2.61%, occur in the core part of the network (part 1). Devices in part 1 are mostly doubled, which means redundancy and fault-tolerant characteristics. On the contrary, there are no redundancies related to devices in parts 2 and 3. Therefore, each fault in these parts causes service failure. Early detection and diagnosis of network element outages that appear in the access part (part 2) of a broadband network is the subject of research presented in this paper.

In most cases, a network element outage leaves a clear trail in fault management logs. Moreover, it is possible to distinguish common sequences of reported failures from much intensive reporting that occurs during a network element outage that has affected a larger group of customers. Figs. 2 and 3 depict the daily number of failures reported by customers related to two DSLAMs in the network during the whole year. Fig. 2 shows common situations that happen most of the time, where only minor problems occur on DSLAM during a year and affect particular customers only. On the other hand, Fig. 3 shows an example where DSLAM outages happened 4 times in a year, seriously affecting services offered to the whole group of customers connected to it. For example, in the Croatian T-HT network there are approx. 6000 DSLAMs, so outages like those described don't represent rare events.

Early and accurate outage detection and diagnostics are of great importance for telecom operators because they reduce costs and increase customer satisfaction and loyalty.

Generally, the accuracy of network element outage recognition can be increased by minimizing missed detection, i.e. false negatives. It should be noted that in fault management practice, there are two problems that often reduce accuracy of outages recognition and promptness.

First is an inadequate monitoring system, designed in a way that causes excessive alarm delays and imposes settings of additional criteria on alarm conditions in order to reduce alarm oscillations and to avoid occurrences of alarm storms. False alarms create severe problems for telecom operators. For example, a false alarm may result in unnecessarily sending the maintenance staff onsite for troubleshooting and divert them away from the real faults. False alarms may trigger unneeded actions to be taken on equipment such as resetting, which cause interruption of the customer's service even when it is not necessary. Therefore, wrong decisions, as a consequence of the false alarms, cause incorrectly

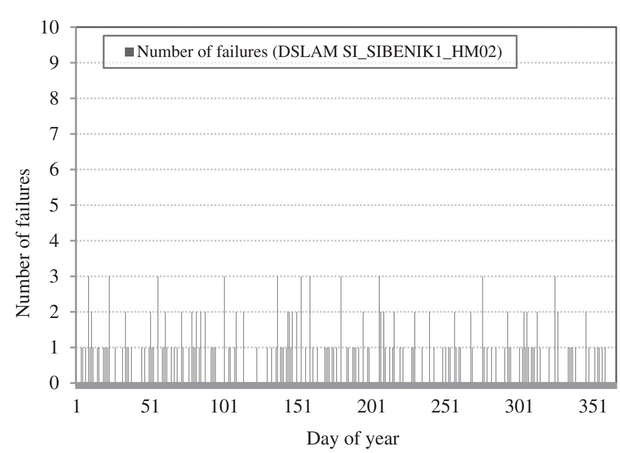

Fig. 2. Reported failures on DSLAM in one year; operation without outages.