Int. J. Electron. Commun. (AEÜ) 77 (2017) 27–35

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

Regular paper

Network failure detection based on correlation data analysis

Piotr Zych

Warsaw University of Technology, Faculty of Electronics and Information Technology, The Institute of Telecommunications, 15/19 Nowowiejska Str., 00-665 Warsaw, Poland

ARTICLE INFO

Article history:
Received 14 May 2016
Accepted 15 April 2017

Keywords:
Network
Monitoring
Failures
RADIUS
Accounting
Point to Point Protocol

ABSTRACT

For a telecommunication operator, the effective detection of access and aggregation network failures is the key to providing continuous service. Although there are many monitoring systems on the market, analysis has shown that there is no possibility of automatically detecting all failures using standard monitoring systems. In this article, an innovative option for failure detection is proposed, based on correlation analysis of data retrieved in real time from the network. A key source of data is the Remote Authentication Dial-in User Service (RADIUS) which records events giving information about a user's Point-to-Point Protocol (PPP) session state sent to the monitoring system. It is shown here that the proposed solution enables an operator to detect all network events affecting customers. The detection of a greater number of events enables the operator to react quickly to them and to restore services to users as soon as possible, which ultimately improves the quality and continuity of provided services.

1. Introduction

Network failure monitoring is a critical process for every telecommunication operator. It is required to be rapid, able to provide data without delays, and very reliable. These requirements are important, because network failures can affect thousands, and sometimes even millions of customers; in some cases the failure of critical infrastructure may even affect people in different countries. It is clear that the operator must react to these events as quickly as possible [1].

Access and aggregation network operation personnel are responsible for failure monitoring and currently use Network Management Systems (NMS) to detect and react to each failure detected, which is shown by the system as an alarm [2]. NMSs are provided by companies that manufacture the hardware or software deployed in the network. Due to the large number of different types of network element and the diverse array of vendors, the operator is required to manage many different NMSs. In order to resolve this problem, several self-developed systems have been created which unify data from different NMSs or even directly from network elements (NE) [3–6].

There are two possible options for network monitoring: cyclic scanning or retrieval of asynchronous events [7].

The advantage of cyclic scanning is its reliability. The system sends a request to the device and can determine whether a response is generated; it can also analyse the body of the response in the case of a request concerning specific parameter/s. However, scanning can be done only at predefined intervals, and thus there is always a delay in event detection. This disadvantage does not arise when the system is configured to retrieve asynchronous data from the network. In this case, the network elements send information on predefined events without delay [7,8]. However, in this situation there is always uncertainty about data loss during transmission, since many events are handled using UDP (User Datagram Protocol), which does not provide a guarantee of transfer; in addition, this type of monitoring cannot be used to monitor device availability, since if a device shuts down completely, it cannot send an alarm.

Failures in the network can be very complex, and sometimes cannot be detected by analysing a single network resource. The types of monitoring described above use predefined datasets to make decisions on existing failures. These datasets are defined by operational personnel, who decide what constitutes a failure. Some of the more obvious parameters are:

- network element reachability;
- card, port, operational status [9];
- card load, temperature;
- interface load (bandwidth used, compared to that available).

However, when a failure is more complex and is not observable through the analysis of a defined dataset, it will not be detected. This generally causes difficulty for the operator since it will eventually be detected through customer complaints. If the failure is detected by the monitoring system, however, the operator can

E-mail address: p.zych@tele.pw.edu.pl

http://dx.doi.org/10.1016/j.aeue.2017.04.014
1434-8411/

react to it almost immediately; thus, before customers report the problem, repair actions will already be in place on the operator side. The earlier a failure is detected, the less impact there is on service provision and ultimately on customers.

It must be assumed that because of the current network complexity (virtual networks in a virtual network, cascading over different technologies, etc.) there is no possibility of defining and monitoring every parameter in a standard way, to be 100% sure of detecting every failure on the network, even with adaptive systems such as those described in [1]. For example, a failure can be caused by the wrong configuration of different network elements, so that traffic cannot be sent between them, while from the point of view of each device everything is configured properly. There is thus a need for an additional monitoring level which will provide general failure monitoring and deliver reliable information about the existing failures in the network.

In the later sections of this article, a new method for failure detection is proposed. None of the current solutions on the market provide the same functionalities as this proposed solution. One similar method is that in [10], which describes failures in the graph architecture of the network; however, there is no specialised focus on the PPP and RADIUS protocols or even the access network, on which the solution proposed in this article is based. In addition, the solution presented by these authors is not focused on correlational data analysis.

There is also US patent [11], which in the author's opinion is one of the closest methods to the proposed solution. This patent defines a process of failure detection based on the number of requests from an alternative location before or after the failure event. A defined threshold must be exceeded in order to trigger the failure event. This patented solution focuses on web applications and queries to the DNS name servers. The similarity to the solution proposed here arises from the triggering of an alarm after exceeding a threshold from the same location; however, the patented solution is not related to access or aggregation networking, its architecture, used protocols or common behaviour.

There are many other articles and patents on the market such as [12–15], although these are all focused on a specific network and its behaviour. Moreover, many of these describe how to compensate for a failure temporarily, for example by switching traffic to another node in the cluster network. In the aggregation network architecture presented in Fig. 2 there is no possibility for switching traffic to other direction; the only solution for minimising damage from failure is to detect this as quickly as possible and to perform manual repair to restore its operational state. In addition, there is no solution which strictly addresses the access and aggregation network failures using the PPP and RADIUS systems (the main purpose of which is not failure detection, but the provision of services) and correlation of data from these systems with knowledge about network architecture.

Network resilience is an important domain to be taken into account when analysing network failures. One of the disciplines within the area of network resilience is network fault tolerance, which defines the ability of the network to work despite a failure. The paper in [16] defines and analyses the *probability of disconnection* in a family of regular graph network topologies; it also introduces the factors of *network resilience* NR(p) and *relative network resilience* RNR(p) as probabilistic measures of network fault tolerance. The definition of NR(p) is the number of failures a network can sustain while remaining connected with a probability (1 – p). The analysis carried out by the authors showed that network resilience increases with network size in regular graphs; however, if the degree of the graph is constant, RNR(p) is a function which decreases with increasing N.

Ref. [17] also discusses network resilience topics; it defines operational metrics N_k and divides them into three groups: normal operation, partially degraded, and severely degraded. The second parameter used is service state, P_k, which is defined as a group of parameters describing the operational state of the services in the network. The business values of P_k are divided into three groups: acceptable, impaired, and unacceptable. Together, N_k and P_k represent the state of the network state $S_k = (N_k, P_k)$. Network resilience

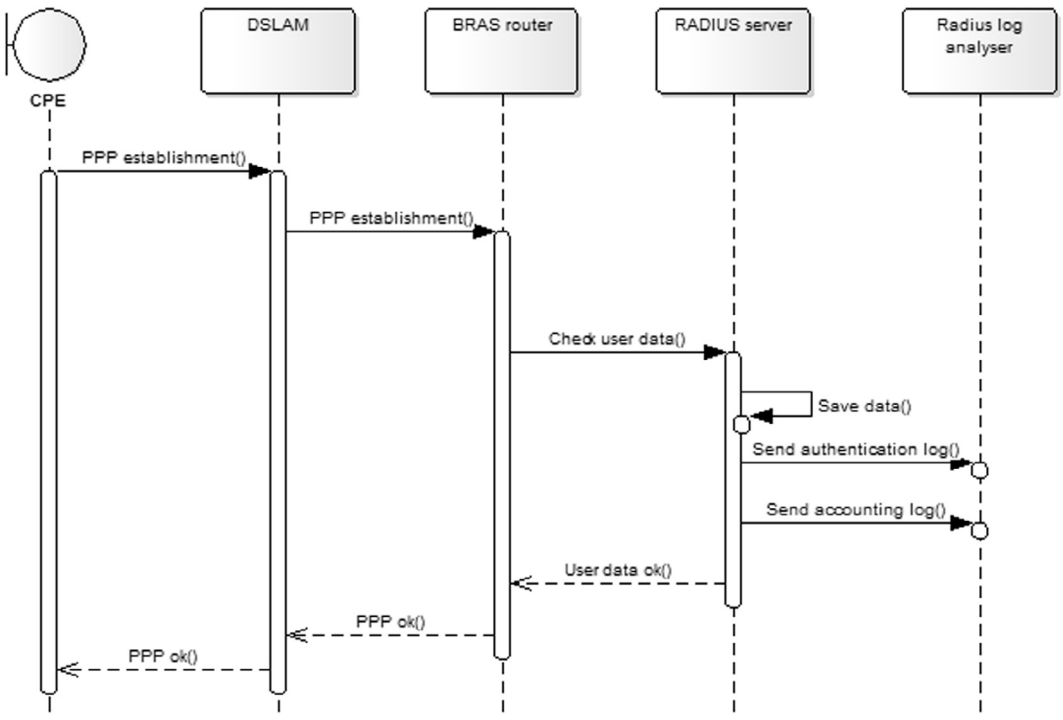

Fig. 1. Establishment of the PPP session and RADIUS log generation.