Opsawg Working Group
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

X. Ding
W. Liu
Huawei
C. Li
China Telecom

October 30, 2017

Network Data Use Case for Wavelength Division Service
draft-ding-opsawg-wavelength-use-case-00

Abstract

This document describes use cases that demonstrate the applicability of network data to evaluate the performance of wavelength division service. The objective of this draft is not to cover the wavelength division service in detail. Rather, the intention is to illustrate the requirements of network data used to evaluate the performance of wavelength division service.

General characteristics of network data and two typical use cases are presented in this document to demonstrate the different application scenarios of network data in wavelength division service.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 3, 2018.

Copyright Notice

Table of Contents

1. Introduction

Wavelength-division multiplexing (WDM) is a method of combining multiple signals on laser beams at various infrared (IR) wavelengths for transmission along fiber optic media. A WDM system uses a multiplexer at the transmitter to join the several signals together, and a demultiplexer at the receiver to split them apart. During the wavelength division service running, network data is consistently generated from wavelength division devices and it can reflect the process of service running.

In the case of wavelength division service, customer is accustomed to handle the network failure after the service interruption. Such passive strategy is inefficient, and easily leads to long service interruption. Network data collected from device is real and reliable, and can help customer to predict the trend of wavelength division optical performance. Statistical characteristics of network data can help operator to judge the time point at which the service is abnormal or normal, or the service is risky or healthy .

This document attempts to describe the detailed use cases that lead to the requirements to support wavelength division performance evaluation. The objective of this draft is not to cover the wavelength division service in detail. Rather, the intention is to

illustrate the requirements of network data used to evaluate the performance of wavelength division service.

General characteristics of network data and two typical use cases are presented in this document to demonstrate the different application scenarios of network data in wavelength division service. Moreover, the question of how to integrate network data collected from different time periods is raised.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

KPI: Key Performance Indicator. Network KPI represents the operational state of a network device, link or network protocol in the network. KPI data is usually represented to users as a set of time series

(e.g., KPI = x_i, i=1..t),

each time series is corresponding to one network KPI indicator value at different time point during specific time period.

3. Characteristics of network data

Network data describes the process that information collected from various data sources and transmitted to one or more receiving equipment for analysis tasks [I-D.ietf-wu-t2trg-network-telemetry]. Analysis tasks may include event correlation, anomaly detection, risk detection, performance monitoring, trend analysis, and other related processes.

Network data is a series of data points indexed in time order. It taken over time may have an internal structure (such as, trend, seasonal variation, or outliers). Trend means that, on average, the measurements tend to increase (or decrease) over time. Seasonality means that, there is a regularly repeating pattern of highs and lows related to calendar time such as seasons, quarters, months, days of the week, and so on. In regression, outliers are far away from the line. With time series data, outliers are far away from the other data.

Network time series data analysis comprises methods for analyzing time series data in order to extract meaningful statistics and other characteristics of the data.

Network data mainly consists several major characteristics:

- Subject: The subject is the object to be measured, and it has multiple properties from different dimensions. An example of a wavelength division service performance monitoring scenario is that the subject of the measurement is the ’ optical module ’ whose attributes may include board name, device name, and so on.

- Measured values: A subject may have one or more measured values, and each measurement corresponds to a specific indicator. Take the server status monitoring scenario example, the measured indicators may have FEC_bef (Forward Error Correction coding before error correction), FEC_aft (Forward Error Correction coding after error correction), input optical power, output optical power, etc.

- Timestamp: Each report of the measured value will have a timestamp attribute to indicate its time.

4. Use cases

The following sections highlight some of the most common wavelength division use case scenarios and are in no way exhaustive.

4.1. Anomaly detection

In Data Analytics Engine, anomaly detection is the identification of items, events or observations which do not conform to an expected pattern or other items in data. Typically the anomalous items will translate to some kind of problem, such as optical layer problem.

For network equipment performance anomalies, multiple features are usually extracted from KPI data, such as time, value, frequency, etc., and used as the key factors for anomaly analysis.

Take wavelength division service as an example, collection information such as FEC_bef, input optical power, laser bias current and other key factors can be selected to keep track of wavelength division service over time and calculate the device statistics data in a specific time period such as average device downtime in the specified time window. These statistics data can be further used to detect wavelength division service anomaly or improve the accuracy rate for wavelength division KPI anomaly detection. In this scenario, we do not rely on the manual preconfigured threshold to trigger alarm, instead, we automatically detect KPI anomaly in advance and raise alarm, as seen in figure 1.

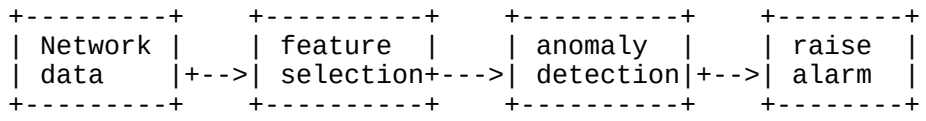

Figure 1: anomaly detection

4.2. Risk assessment

In Data Analytics Engine, risk assessment is a component aiming at providing an estimation of the overall network risk condition. Unlike the anomaly detection component that copes with network faults and failure that already happened, risk assessment module's goal is to anticipant network event, forecast short term change and risk in the network based on the trends of network data (e.g., fast growing, fast dropping, slowly increasing, and slowly decreasing of KPI data). This opens up a channel to reveal potential network problems or locate the need for network optimization and upgrade.

Network KPIs provide fine-grained understanding of network performance, which bring more value to network maintenance and operation, including identifying possible bottlenecks, dimensioning issues, and locating the need to perform network optimization. Based on the various monitor mechanisms, if any high risk is occurred in the network, administrators could be informed at a very early stage. The ability to handle large amount of noisy KPI data properly is vital to gain these desired insights.

Given hundreds of thousands of KPI data, it is a challenging issue to assess network risk. Good network risk assessment criteria should be indicative of local network-level problems, and hence be able to provide prompt warnings and help locate potential problems when trivial but persisting anomalies are observed. Meanwhile, it must also describe system performance in a global sense by aggregating multi-faceted information with large number of KPIs across the network infrastructure. There are two strategies to design such KPI network risk, as shown in figure 2:

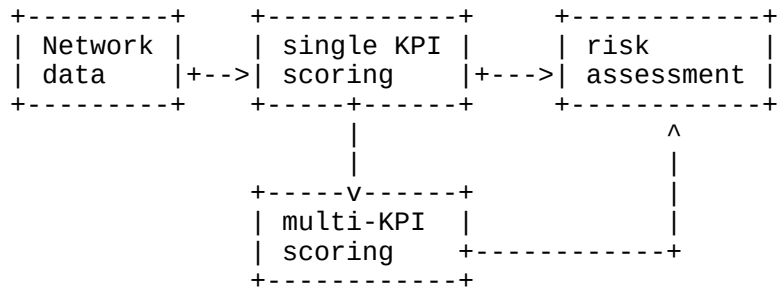

Figure 2: risk assessment

1) Single KPI scoring: The scoring strategy for single KPI. In this case, different dimensions of a KPI should be examined to score a KPI;

2) Multi-KPI scoring: The scoring strategy for assessing the network risk using values of many KPIs. If a device or a service is monitored by several key KPIs, the risk should be analyzed by the integration of these KPI scores.

5. Data Issues

5.1. Merge data from different time periods

In the process of data collection, the collection period of the same KPI may be different from each other. For example, for a multi-domain deployment service, there are many different collection periods for network devices, such as 30s, 5min, 15min, and so on.

KPI data collected from different domains is need to be analyzed for correlation. For example, anomaly detection of wavelength division service data from different domains is performed, and comparison is performed among different domains. So we need to merge data sets from different periods into a integrated data set using metrics in the period, such as mean value, peak value or media value. It then raises a question that how these data sets are stored and assessed with high efficiency.

6. Security Considerations

TBD.

7. Conclusions

TBD.

8. Normative References

[I-D.ietf-wu-t2trg-network-telemetry]
Wu, Q., "Network Telemetry and Big Data Analysis", March 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

Authors' Addresses

Xiaojian Ding
Huawei
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Email: dingxiaojian1@huawei.com

Will(Shucheng) Liu
Huawei
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com

Chen Li
China Telecom
No.118 Xizhimennei street, Xicheng District
Beijing 100035
P.R. China

Email: lichen@ctbri.com.cn