Technical Disclosure Commons

Defensive Publications Series

August 13, 2018

INTELLIGENT TELEMETRY DRIVEN NETWORK

Ashish Ravindranathan

Abhijith B.R

Rajesh Kumar Madabhattula

Sunil C

Recommended Citation

Ravindranathan, Ashish; B.R, Abhijith; Madabhattula, Rajesh Kumar; and C, Sunil, "INTELLIGENT TELEMETRY DRIVEN NETWORK", Technical Disclosure Commons, (August 13, 2018)
https://www.tdcommons.org/dpubs_series/1404

INTELLIGENT TELEMETRY DRIVEN NETWORK

AUTHORS:
Ashish Ravindranathan
Abhijith B.R
Rajesh Kumar Madabhattula
Sunil C

ABSTRACT

By streaming real-time Optical Transport Network (OTN) and optical performance parameters from network devices using telemetry, the values of the next few intervals may be forecasted. Proactive alerts may be provided to the users and corrective action may be taken if the user chooses. Possible impact to millions of users riding the system may thereby be avoided. This provides a seamless experience to the users.

DETAILED DESCRIPTION

Bandwidth demands have grown multi-fold. Today, optical Dense Wavelength Division Multiplexing (DWDM) networks have become the backbone of the transport layer to cater to the high demands. In these systems, one 100G wavelength can carry about 1.1 million to 3.1 million voice users/calls depending on the particular codec in use. DWDM systems can carry 32, 40, 80, 96 or more such 100G/200G wavelength over a fiber pair depending on the particular configuration in use.

In such systems, when there is a complete fiber cut it is easy for service providers to identify the fault. However, in case of degradation not amounting to a complete fiber cut/failure, the problem usually goes unnoticed until the end user reports quality degradation in the service. The service providers may then begin troubleshooting the circuit path to isolate the issue by looking at available alarms and variations in performance reports. Much time is lost in this reactive process, which impacts the time to restore and drastically decreases user experience. The time required and complexity increases multi-fold with the increase in the number of nodes/spans involved in the circuit path.

Another issue is that performance reports are usually available with approximately fifteen-minute intervals. Sharp variations may occur for a few minutes, become averaged out, and therefore not provide a clear real-time picture.

There are parameters in Optical Transport Network (OTN) performance (e.g., Optical Signal to Noise Ratio (OSNR), pre - Forward Error Correction (FEC) Bit Error Rate (BER), receive power, etc.) of the trunk port and optics performance that would see variations when there is any hardware/software failure or link degradation in the path. These parameters are monitored real-time using telemetry data and the values of these parameters are forecasted for the next few intervals.

Link degradation can have various causes, such as fiber pull/damage due to road works, extremes in weather temperatures causing fluctuations in the fiber, high winds which cause fluctuations in aerial fibers, fiber impairment added due to excessive stress on low trench fiber ducts, pinched/pulled fiber patch cords, fiber damage due to rodents, temperature variations at end equipment sites the cause the lasers used in transponder cards to stray away from the center frequency, laser degradation due to aging of the laser on end transponder cards, any hardware/software failure affecting transmit ports, etc.

Currently, there are no known optical DWDM systems that are able to forecast a possible customer impacting link degradation. The techniques presented herein enable detecting and forecasting effectively all kinds of link degradation issues before millions of users are impacted. The model continuously relearns and updates the transition states probabilities.

Static thresholds have been proven not useful. The current approach to detect degradation is by setting a Threshold Crossing Alert (TCA) for OTN performance parameters. Although these old reactive approaches have been used for a long time, these alerts typically would be raised when the user would have already started experiencing an impact due to the degradation. If the TCA thresholds are set lower to get alerts before an impact, then many false positives are raised and these alerts get lost in floods of alarms in medium/large size networks.

The techniques described herein do not rely on static thresholds. Rather, this model understands a user profile based on the monitored parameters and, when it observes a declining trend, it identifies an anomaly before a cut off value is reached. For example, assume the normal pre-FEC BER in one user scenario hovers around 10-8. If the value begins decreasing but the threshold for raising the alert has not been reached, such a trend should be identified and a proactive alert should be provided to service providers.

The techniques described herein enable forecasting a possible user impacting link degradation and proactively alerting the service provider. Rather than raising the alert after crossing a threshold, the user may be informed that the threshold is going to be crossed at 'x' intervals from now. This is a proactive/predictive, not reactive, approach.

The user configures the network devices to stream real-time telemetry data to a collector server. This can be done by creating a subscription for the relevant sensor paths so that real-time telemetry data from the devices can be streamed to the collector server. The user can select the trunk port/s to be monitored by the optical transport devices, the port on which corrective action is to be taken, and the type of corrective action. Corrective actions may include monitoring only, sending alerts only, and/or sending alerts and shutting down the selected port/s. Based on this selection, a Telemetry Data Agent may parse the telemetry data for the required ports.

An Anomaly Forecast Model may consume this real-time data and forecast the values of next few intervals of a thirty second period and persist the values into a time series database (e.g., InfluxDB). A graphical representation of this real-time and forecast data for the selected ports may be viewed at any point in the real-time dashboard. If the model predicts that the upcoming values will impact the user, the model may flag this result and send a proactive major alert with the time stamp of the expected anomaly. After several more intervals have passed, if the model still sees no improvement in the forecast, it may send out a critical alert to the user and take corrective action as per the user selection. Thus, the user is not impacted and has a seamless experience.

Figure 1 below illustrates this process.

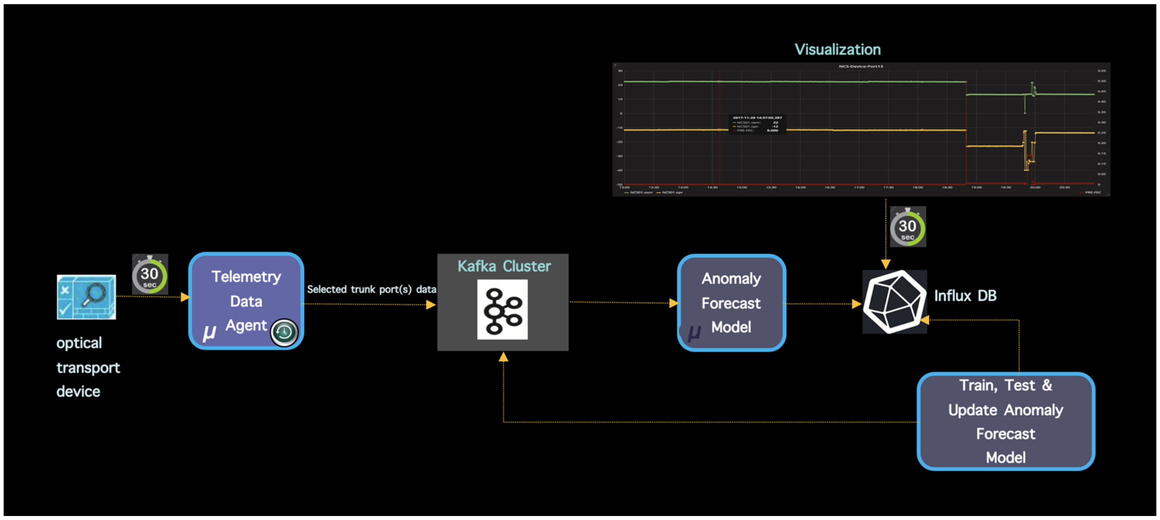

Figure 1

With respect to the anomaly forecast model, the trunk port parameters start in state s0 and stochastically transition from state to state. At each time unit, the trunk port emits a multivariate observation and then transitions to another state (e.g., s1, s2, etc.), which indicates that some variation has occurred in the underlying transport path. Some random trajectory of states over time produce another multivariate observation sequence. Successive state paths and the multivariate emission sequences produced by different variations of trunk ports may generally be different since the operation of the transport path is stochastic. As such, not all states are visible. The states that are emitted during link degradation are different from normal states. There may also be multiple states during link degradation as well depending on the particular reason for degradation. The model may learn all states, including hidden states, and predict the next states with some probability. The model may continuously relearn and update the transition state probabilities.

Figure 2 below illustrates an example lab setup diagram of a working prototype. In this setup, two routers are connected via two 10 Gigabit Ethernet ports that are in an ether channel bundle. One Virtual Machine (VM) is connected to each routers. In the transport path, an optical transport device has 10G client ports and a 100G DWDM trunk port, and another optical transport (DWDM) device is connected via seventy-five kilometers of fiber spool. One 10G link connects the routers via the top 100G link (passing through the optical transport DWDM device path), and the other 10G link connects the routers via the bottom 100G link. Multicast video traffic is streamed from the left VM to the right VM. To simulate fiber degradation the variable optical attenuator is manually increased. Trunk port

0/0/0/13 on the right optical transport device is monitored. When the model forecasts an end user impact, it shuts down this trunk port, thereby removing it from the EtherChannel bundle. Thus, the video streaming of end user is not affected.

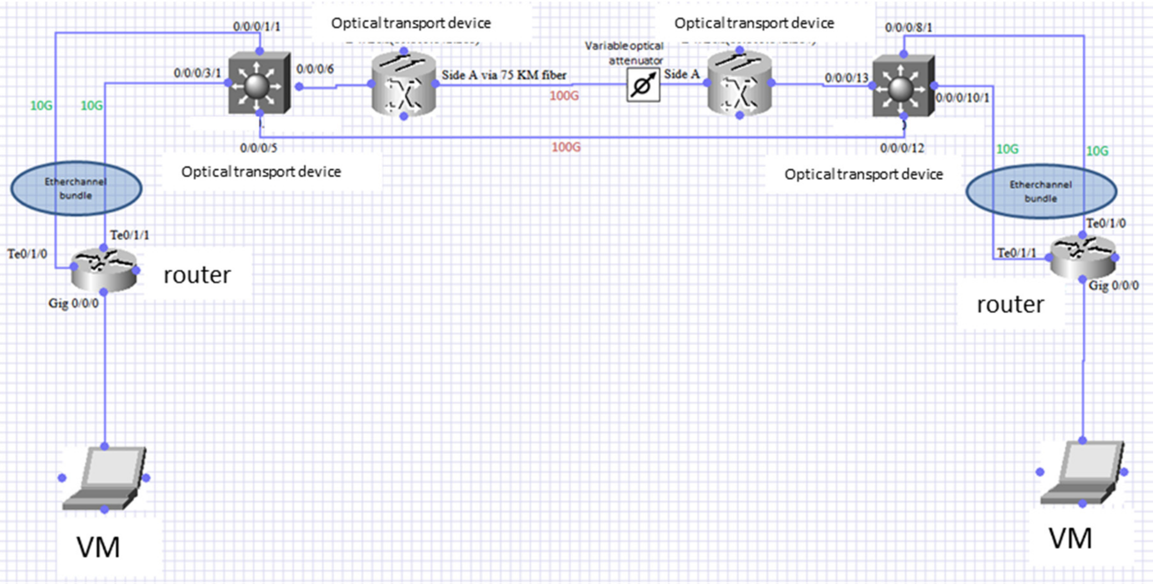

Figure 2

The failures in the optical network may be forecasted and the downtime of millions of users that utilize the optical DWDM systems may be reduced. The troubleshooting time for service providers may be reduced, and the users may thus have a seamless experience. Since trunk ports are being monitored, any failure may be predicted, regardless of whether the failure is due to hardware/software or physical path degradation failure (e.g., starting from the other end transmit port, to any pinched patch cords anywhere in the path, any issue with Reconfigurable Optical Add Drop Multiplexer (ROADM) in the path or any fiber degradation in the path, etc.).

In summary, by streaming real-time OTN and optical performance parameters from network devices using telemetry, the values of the next few intervals may be forecasted. Proactive alerts may be provided to the users and corrective action may be taken if the user chooses. Possible impact to millions of users riding the system may thereby be avoided. This provides a seamless experience to the users.