Optical Network Anomaly Detection and Localization Based on Forward Transmission Sensing and Route Optimization

Philip N. Ji[1], Zilong Ye[1,2], Yue-Kai Huang[1], Thomas Ferreira de Lima[1], Yoshiaki Aono[3], Koji Asahi[3], and Ting Wang[1]
[1]NEC Laboratories America, 4 Independence Way, Princeton, NJ 08540, USA
[2]California State University Los Angeles, 5151 State University Drive, Los Angeles, CA 90032, USA
[3]Transport Network Department, NEC Corporation, Abiko, Japan
pji@nec-labs.com

Abstract: We introduce a novel scheme to detect and localize optical network anomaly using forward transmission sensing, and develop a heuristic algorithm to optimize the route selection. The performance is verified via simulations and network experiments.

1. Introduction

Fiber optic sensing offers many benefits compared to traditional discrete mechanical or electrical sensors, such as high sensitivity, immunity to EMI, and robustness. As a result, it has been applied to a growing number of applications. Recently, existing fiber optic communication networks are utilized as the sensing media (called "Network-as-a-Sensor" or NaaSr) [1], further reducing the deployment cost and time, and making fiber sensing even more attractive.

Conventional fiber sensing technologies and sensors rely on the backscattering of incident optical pulses, namely the Rayleigh, Brillouin, and Raman backscattering. Even though they offer high sensitivity and the ability to localize the event with fine spatial resolution, the combination of round-trip operation and weak backscattering signal limits their maximum sensing distance. State-of-the-art commercial fiber sensing equipment can only reach ~100 km. In addition, the mismatch of optical power levels makes it difficult for sensing and communication signals to coexist on the same fiber. Furthermore, the isolators inside optical amplifiers block the backscattering light, which prevents backscattering-based sensing from multi-span application in telecom networks.

Recently, forward transmission-based sensing technologies have been proposed and demonstrated [2-5]. They do not rely on optical backscattering. Instead, the temporal variation of optical characteristics, such as state of polarization (SoP) or phase, are measured to detect the physical events/anomalies occurred on the fiber. This allows long distance sensing over existing telecom networks, such as seabed earthquake detection via >10,000 km transoceanic fiber optic network [3]. Besides achieving long distance sensing, forward transmission sensing systems can work seamlessly with the amplifiers and other WDM channels in the network. Some of them even use existing telecom transponders to obtain the SoP or phase information, which further reduces the hardware cost and spectrum resource. On the other hand, the drawback of forward transmission sensing is that the technique itself cannot identify the anomaly event location, as no round trip time-of-flight information is obtained. Several techniques were recently proposed to solve this issue, including bidirectional transmission [4] or repeater loopback [5]. However, they require complex system modification and high-cost hardware components, and still can only deliver limited localization capability.

Most terrestrial metro and long-haul optical networks are not just a point-to-point link, but contain multiple nodes and links connected in different topologies. In many network monitoring applications, identifying which link the anomaly occurs is sufficient, or provides the first essential step. In this work, we propose a scheme to detect and localize anomaly in large-scale optical networks using forward transmission sensing, and we develop a heuristic algorithm to optimize the route selection. The performance is verified via simulations and network experiments.

2. Network anomaly detection and localization based on forward transmission sensing

The proposed network anomaly detection scheme is based on forward transmission sensing and network-wide global planning of the sensing routes. Firstly, multiple sensing routes are selected to cover the entire network and each link in the network is guaranteed to be passed by a different combination of sensing routes. These routes are then monitored concurrently and analyzed centrally. When an anomaly event occurs at a specific link, the receivers in the corresponding routes will detect the optical characteristic change. Since the sensing route combination is unique for each link, the global analysis of the optical characteristic change will indicate the exact link that causes the event.

Figure 1 shows an example of a mesh network with 5 nodes and 7 links. Three sensing routes are set up as shown in Fig. 1 and Table 1. With this arrangement, each link is associated with a unique combination of sensing routes. Three of the links (AD, CE, and DE) are traversed by three unique routes. Three other links (AB, BC, and BE) are traversed by two unique sets of routes, and the last link (CD) has all three routes overlapped. When an event occurs on a specific link, the receiver at the corresponding routes will report abnormal optical characteristics, as indicated by 1's in Table 1, otherwise it is shown as 0. For *N* routes, an *N*-digit binary code will thus be formed. The route selection

ensures that each link has a unique code, which can easily localize the link if an event occurs. For example, if an anomaly occurs at link BC, the code 011 will be obtained since Route 2 and Route 3 will report the abnormal optical characteristics and Route 1 will not. From this "011" code, the anomaly event at link BC can be instantly identified.

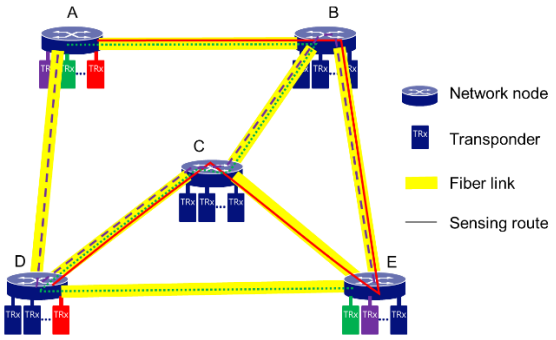

Fig. 1. Network anomaly detection example

Table 1. Event code and identification table

Route 1 (A-B-E-C-D)	Route 2 (A-B-C-D-E)	Route 3 (A-D-C-B-E)	Indicating event at
0	0	0	No event
0	0	1	AD
0	1	0	DE
1	0	0	CE
0	1	1	BC
1	0	1	BE
1	1	0	AB
1	1	1	CD

3. Sensing route optimization algorithm and analysis

To apply this anomaly detection and localization scheme, it is desirable to keep the number of sensing routes to the minimum while still covering the entire network with per-link identification capability. For a network with N links, the trivial upper bound is N routes, but this is not efficient. The theoretical lower bound is $\lceil \log_2(N+1) \rceil$, since it needs to differentiate among N links and the "no event" case. Here, we do not consider the case of simultaneous multiple events, since it is rare that anomaly occurs on more than one link at the same instant of time. As long as there is a brief time gap between two events, they can be identified and localized one at a time. The example in Fig. 1 shows the theoretical lower bound case of 3 routes when N is 7. However, this theoretical lower bound is seldom achievable since it only works on specific network configurations. Here, we develop a novel heuristic algorithm to find the optimal route selection for any network configurations or topologies.

The proposed heuristic algorithm aims at assigning the minimum number of sensing routes such that (1) each link is sensed or covered at least by one sensing route and (2) each link is associated with a unique binary code (corresponding to a unique combination of sensing routes) that is not all 0s (which indicates no anomaly event). Here, the code between different links are required to be non-identical, so that the anomaly event can be localized immediately. The proposed heuristic algorithm is a greedy algorithm that consists of four steps. Firstly, it applies breadth-first search to obtain all the routes that are originated from each node with a maximum of k hops. Secondly, a matrix T with links as rows (N rows) and all the routes as columns (M columns) can be constructed, as shown in Table 1. Here, $T[i][j]$ is 1 if route j passes through link i; 0 otherwise. Thirdly, the algorithm examines each route and selects the one that introduces the minimum number of identical code between links for deploying a new sensing route. This step repeats until there is no identical code between different links. Finally, after the above iteration is complete, if one of the links has a code consisting of all 0s, a new sensing route (only one hop) will be deployed to just cover this particular link. This is because, even if all 0s is a unique code, it represents there is no abnormal optical characteristic change found at any route, which cannot be used as the code for identifying anomaly event at any link.

We also develop an integer linear programming (ILP) model to obtain the optimal solution. We assume that M routes are found using the breadth-first search. A variable δ_k ($k \in M$) is defined to be 1 if route k is selected for deploying sensing route; 0 otherwise. The objective is to minimize the number of sensing routes, which is defined as:

$$\min \quad \sum_{k=1}^{M} \delta_k$$

$$\text{s. t.} \quad \sum_{k=1}^{M} |T_{i,k} \cdot \delta_k - T_{j,k} \cdot \delta_k| \geq 1 \quad \forall i \in N,\ j \in [i+1,\ N] \qquad (1)$$

$$\sum_{k=1}^{M} T_{i,k} \cdot \delta_k \geq 1 \quad \forall i \in N \qquad (2)$$

Here, Eq. (1) ensures that the code for each link is unique, so that any anomaly can be localized immediately. Eq. (2) guarantees that each link's code contains at least one 1, which means that a link is covered by at least one sensing route. Here, Eq. (1) is non-linear, which is not directly solvable. We define an auxiliary matrix A that has three dimensions, where $A[i][j][k]$ is 1 if $T[i][k]$ is equivalent to $T[j][k]$ (meaning that links i and j have identical code at bit k when route k is selected); 0 otherwise. Then, the first constraint can be transformed to Eq. (3), which becomes linear and is solvable.

$$\sum_{k=1}^{M} A_{i,j,k} \cdot \delta_k \geq 1 \quad \forall i \in N, j \in [i+1,\ N] \qquad (3)$$

Compared to the heuristic algorithm, the ILP solution sets up the practical lower-bound benchmark. However, it may not be tractable when the network size is large.

We conduct a set of comprehensive simulations to evaluate the performance of the proposed greedy algorithm and the ILP solution. The upper bound N is also listed for comparison. Firstly, we evaluate the number of sensing routes

used across different real-world optical networks [6], using breadth-first search for routes with a maximum of 4 hops. The results are shown in Table 2. We can see that the greedy algorithm achieves a performance that is close to the optimal solution obtained by the ILP model. As the network size increases (e.g., Palmetto, ION, USC), the proposed greedy algorithm continues to achieve an efficient performance, while ILP cannot yield to a solution. Furthermore, the idea that more available routes may give us a better pool of sensing routes motivates us to evaluate how the maximum number of hops k may affect the performance of the greedy algorithm. As shown in Table 3, as the maximum hops k increases (which introduces more available routes to the pool), the number of sensing routes used by the greedy algorithm decreases. If we cross compare the ILP results in Table 2 and the greedy algorithm results in Table 3 for the networks of Oxford, INS and Valleynet when the maximum hop is 6, we can observe that the greedy algorithm achieves the same performance as the optimal solution obtained by ILP. This demonstrates that the proposed greedy algorithm can achieve close-to-optimal performance when the maximum hop k is large.

Table 2. Greedy vs. ILP vs. Upper bound

	Oxford	INS	Valleynet	Palmetto	ION	USC
Upper bound N	24	28	33	63	92	166
Greedy	13	15	18	30	55	91
ILP	10	12	15	*	*	*

*: unable to yield a result in a reasonable amount of time

Table 3. The effect of the maximum hops k

k	Oxford	INS	Valleynet	Palmetto	ION	USC
2	18	21	25	48	69	126
3	15	17	19	37	60	104
4	13	15	18	30	55	91
5	12	13	16	26	54	86
6	10	12	15	23	51	81

4. Network anomaly detection and location experimental verification

The feasibility of this scheme is verified experimentally. We set up a 5-node network with the same topology as the example in Fig. 1. The optical channels are set up using commercial 400GbE whitebox transponders, which are compliant with Telecom Infra Project's (TIP's) Phoenix requirements, consists of the NEC Network Operating System (based on the open-source Goldstone software) running on Wistron's Galileo Flex-T hardware with Lumentum 400GbE CFP2-DCO pluggables. Six DCO modules are used in this experiment to set up communication on three routes, with three used as transmitter and three as receiver. The maximum SoP rotation speed is reported by each receiver transponder every second, which is used as the monitoring parameter. The transmission quality of each route is monitored by the built-in pre-FEC BER readouts from the DCOs, which are also updated every second. 4 THz wide optical ASE signal is added through a wavelength-selective switch (WSS) to emulate other WDM channels. The links contain multiple fiber spools with standard single mode fibers (SSMF) between 20 km and 80 km, and short sections of multi-strand optical cable when multiple routes converge. The nodes consist of WSS and optical amplifiers.

During the experiment, shaking, twisting, or bending actions are applied to each link to emulate anomaly events. Each action lasts 2 to 4 seconds. The SoP speed on all three routes are read concurrently. Fig. 2 shows the three SoP speed curves in 50-second windows under different actions. A threshold of 500 rad/sec is set to determine whether an anomaly occurs. The combed analysis results from three channels forms the binary code that instantly indicates the link where the anomaly occurs. The experiment results match well with the expectation. For example, when a section of link BE is shaken in Fig. 2(f), both Routes 1 and 3 experience large SoP change, while the SoP at Route 2 remain normal (well below the threshold). During the operation, all transponders continue to transmit data error-free.

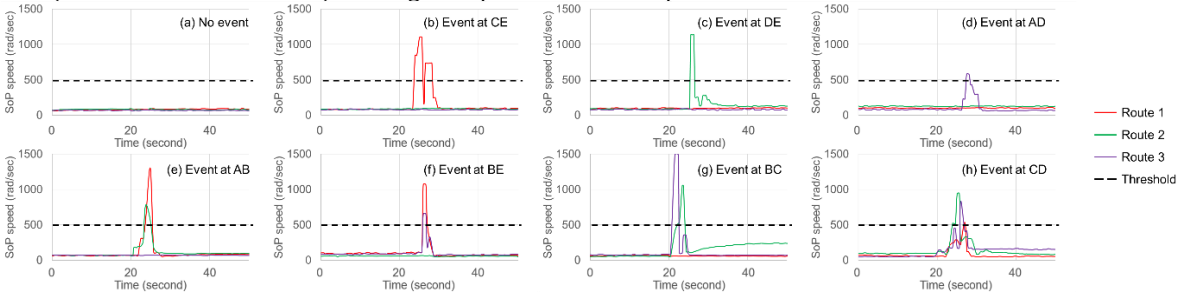

Fig. 2. Measured SoP speed curves under different network events

5. Conclusions

We introduce and experimentally demonstrate a forward transmission sensing-based network monitoring and anomaly detection solution. A close-to-optimum heuristic algorithm is developed for sensing route selection. This solution can efficiently detect and localize otherwise invisible physical anomalies in large-scale optical networks and provide advance warning before any anomaly causes transmission quality deterioration or fiber cut, therefore it has great potential for network application.

[1] Z. Ye, et al., ECOC 2020, We2K-4.
[2] G. Marra, et al., Science **361**, 486-490 (2018).
[3] M. Cantono, et al., ECOC 2020, Th2H-2.
[4] E. Ip, et al., J. of Lightwave Tech. **40 (5)**, 1472-1482 (2022).
[5] F. Yaman et al., SubOptic 2023, We3A-4.
[6] http://www.topology-zoo.org/dataset.html