On Multi-Layer Restoration in Optical Networks with Encryption Solution Deployment

Xin Jin[1], Wei Lu[1], Siqi Liu[1], Zuqing Zhu[1]

1. University of Science and Technology of China, Hefei, Anhui 230027, China, Email: zqzhu@ieee.org

Abstract: We consider the scenario in which an optical network with encryption solution deployment can be affected by electrical layer failures, and propose an algorithm to improve the cost-effectiveness of multi-layer restoration in it.

OCIS codes: (060.1155) All-optical networks; (060.4251) Networks, assignment and routing algorithms.

1. Introduction

With the rapid development of emerging applications, the volume of sensitive traffic delivered with optical networks has been increasing dramatically [1]. However, there are physical-layer vulnerabilities in optical networks, which can be leveraged by malicious users to realize wire-tapping that is difficult to be detected [2, 3]. This motivates people to study physical-layer encryption technologies that can directly encrypt data in the optical transport networking (OTN) payload frames, for achieving the advantages such as low latency and small overhead [1]. Meanwhile, the network architecture that supports cost-effective OTN encryption solution deployment (ESD) is of great interest, too. Previously, the authors of [4] have analyzed the cost-effectiveness of three network architectures for ESD, and the architectures were based on transparent wavelength-level routing, cross-layer grooming, and translucent point-to-point provisioning (*i.e.*, *Architectures* I, II and III in Fig. 1), respectively. The analysis suggested that *Architecture* II with cross-layer grooming can improve the utilization of linecards (LCs) and encryption cards (ECs) for high cost-effectiveness.

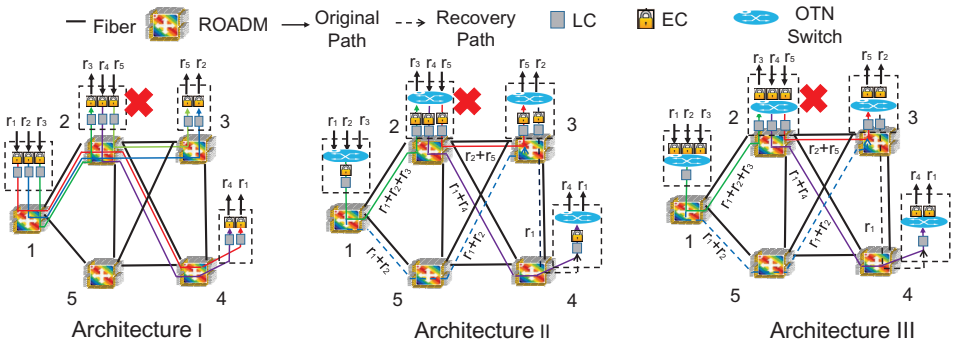
Nevertheless, the analysis in [4] was conducted based on the assumption that the optical network with ESD is always intact, *i.e.*, both the optical and electrical layers in it would not fail. This might not be a practical assumption. Moreover, a recent study on Google's wide-area networks suggested that electrical layer failures actually happened more frequently than those in the optical layer [5]. Hence, it would be relevant to revisit the problem discussed in [4], and to investigate whether the architectures still perform similarly when electrical layer failures have to be addressed[1]. This, to the best of our knowledge, has not been studied before, and in the next section, we will use the intuitive example in Fig. 1 to explain why the investigation is necessary. Note that, to address electrical layer failures, a cost-effective multi-layer restoration (MLR) scheme [6, 7] will be needed. However, the MLR in an optical network with ESD needs to not only modify the operations of the LCs and lightpaths but also readjust the ECs, which has not been considered in previous studies on MLR in optical networks without ESD. Moreover, as we will explain later, the modifications on LCs, lightpaths and ECs in MLR are correlated, which makes the problem even more complex.

In this work, we consider the scenario in which an optical network with ESD can be affected by electrical layer failures, and analyze the three architectures discussed in [4] to reveal their cost-effectiveness in MLR. We first discuss the MLR schemes that the architectures will use to address electrical layer failures. Then, an algorithm is designed to improve the cost-effectiveness of MLR in *Architectures* II and III. Finally, we conduct simulations to compare the architectures' cost-effectiveness in MLR. With the simulation results, we try to answer the question which architecture performs the best in improving the utilization of LCs and ECs when MLR has to be considered.

2. Analysis on Multi-Layer Restoration in Architectures for Encryption Solution Deployment

In Fig. 1, we assume that an electrical layer failure happens on *Node* 2. Note that, this work utilizes the failure categorization discussed in [5], and assumes that an electrical layer failure on a node brings down the OTN switch and all the LCs and ECs on it but leaves the reconfigurable optical add/drop multiplexer (ROADM) intact. Hence, we can see that the failure makes the demands $\{r_3, r_4, r_5\}$ unrecoverable because they use *Node* 2 as their source or destination nodes. In *Architecture* I, the services for $\{r_1, r_2\}$ will not be affected by the failure, since they are switched all-optically in the ROADM. In *Architecture* III, the services for $\{r_1, r_2\}$ will be affected but they can be restored with only rerouting and re-grooming. Specifically, *Node* 1 can change the lightpath for $\{r_1, r_2, r_3\}$ originally to only include r_1 and r_2 and reroute it to *Node* 3, where r_2 is received locally and r_1 is send to *Node* 4 with a new lightpath. Hence, the MLR reconfigures three LCs on *Nodes* 1, 3 and 4, respectively, and uses a new LC on *Node* 3. Since *Architecture* III uses end-to-end encryption, MLR does not need to use new ECs or reconfigure any in-service ECs.

[1] Here, we do not consider the failures in the optical layer (*i.e.*, fiber cuts). This is because a quick check can reveal that as long as each fiber link is protected in the optical network, the architectures perform similarly as discussed in [4] even when there would be optical layer failures.



	# of New ECs	# of New LCs	# of Reconfigured ECs	# of Reconfigured ECs
Architecture I	0	0	0	0
Architecture II	1	1	3	3
Architecture III	0	1	0	3

Fig. 1. Examples on MLR in three architectures for optical networks with encryption solution deployment (ESD).

However, the situation in *Architecture* II is the most interesting and complex among the three. First of all, we notice that the services for $\{r_1, r_2\}$ cannot be restored with only rerouting and re-grooming. This is because originally on *Node* 1, the traffic of $\{r_1, r_2, r_3\}$ is groomed first and then encrypted. Hence, even if we take r_3 out on *Node* 1 and reroute the lightpath to *Node* 3, the services for $\{r_1, r_2\}$ cannot be restored because the ECs on *Nodes* 3 and 4 are not configured correctly. To this end, the MLR in *Architecture* II needs to first reconfigure the LC pair and EC pair on *Nodes* 1 and 3 to reroute the services for $\{r_1, r_2\}$ to *Node* 3, and then set up a new lightpath to send r_1 to *Node* 4. This leads to using a new LC and a new EC on *Node* 3 and reconfiguring the LC and EC on *Node* 4. Hence, in addition to the modifications in *Architecture* III, the MLR in *Architecture* II reconfigures three ECs and uses a new EC.

The table in Fig. 1 summarizes the modifications in the architectures to address the electrical layer failure on *Node* 2, which implies that *Architecture* II would be the least cost-effective. Note that, we only consider the costs of reconfiguring/adding LCs and ECs here, but ignore them due to ROADM reconfigurations. This is because compared with ROADM reconfigurations, reconfiguring/adding LCs and ECs is usually much more complicated and power-consuming. Although the table in Fig. 1 suggest that *Architecture* II is the least cost-effective in MLR, the architecture still uses the least LCs and ECs originally in the normal operation. Hence, we will design an algorithm to improve the cost-effectiveness of the MLR in *Architectures* II and III, and compare the architectures' cost-effectiveness in a comprehensive manner (*i.e.*, considering both the normal operation and the MLR to address electrical layer failures).

3. Multi-Layer Restoration Algorithms in Consideration of Encryption Solution Deployment

We denote the topology of the multi-layer optical network as $G(V,E)$, *i.e.*, $G(V,E) = G_o(V_o,E_o) \cup G_i(V_i,E_i)$, where G_o and G_i are the topologies of the optical and electrical layers, respectively, V_i is the OTN switch set while all the ROADMs are included in V_o, and the virtual links in the electrical layer are in E_i and E_o is the fiber link set. Each traffic flow in the optical network is denoted as $r(s,d,l)$, where s and d are its source and destination, respectively, and l represents its data-rate. As explained above, MLR in the optical network may reconfigure in-service LCs/ECs and use new LCs/ECs. Hence, we define the operational expense (OPEX) of the MLR to restore r as $C^r = n_1 \cdot c_l^s + n_2 \cdot c_l + n_3 \cdot c_e^s + n_4 \cdot c_e$, where c_l^s and c_e^s are the unit costs to reconfigure an in-service LC/EC, respectively, c_l and c_e are the unit costs of using a new LC/EC, respectively, and $\{n_1, n_2, n_3, n_4\}$ are the numbers of corresponding LCs/ECs. Then, we design an MLR algorithm with the procedure below to restore affected flows in *Architectures* II and III.

Step 1 (Obtain Network Status): When an electrical layer failure occurs, we remove the broken OTN switch to generate the new multi-layer topology $G(V,E)$, and find all the affected flows that do not use the broken switch as source or destination. These affected flows are recoverable and we store them in set $\mathbf{R}^a$.

Step 2 (Sort Affected Flows): We sort the affected flows in $\mathbf{R}^a$ in ascending order of their original hop-counts in the electrical layer $G_i(V_i,E_i)$, *i.e.*, the number of lightpaths that each of them uses originally.

Step 3 (Build Auxiliary Graph): For each flow $r(s,d,l) \in \mathbf{R}^a$, we build an auxiliary graph (AG) $G^a(V^a,E^a)$ to find the most cost-effective MLR scheme for it. Here, we have $V^a = V_i$, which includes all the working OTN switches in the updated multi-layer topology $G(V,E)$. Then, for all the virtual links in E_i, we remove those that do not have enough capacity to support r's data-rate l and insert the remaining ones in E^a. These are the virtual links that can be leveraged to restore r. Then, we assign a weight to each link $e \in E^a$, which is the OPEX due to the LC/EC modifications on its end-nodes if we use e to restore r. Note that, the link weight is different in *Architectures* II and III. Next, we add a new virtual link in E^a to connect s and d directly to represent the option of adding a new end-to-end lightpath to restore r,

and the link's weight is also calculated accordingly.

Step 4 (Find MLR Scheme): With the AG G^a, we find the least weighted path in it for $s \rightarrow d$, which represents the most cost-effective MLR scheme to restore r. Then, we restore r accordingly and update the network status in G.

Step 5 (Restore Affected Flows): We repeat **Steps 3-4** until all the affected flows in $\mathbf{R}^a$ are restored.

4. Simulation Results

To re-evaluate the architectures in [4], we perform simulations with a 14-node NSFNET topology [3]. We assume that the capacity of a lightpath is 100 Gbps, and based on the discussions in [1], we set the cost parameters as $c_l^s = 0.24$, $c_e^s = 0.7$, and $c_l = 0.8$, and $c_e = 1$. Here, the unit cost to reconfigure an EC is much higher than that of an LC because when reconfiguring an EC, we need to not only adjust its data-rate but also reassign the encryption key. In each simulation, we first randomly generate a traffic matrix with a fixed total volume of 9.5 Tbps, and serve the traffic flows in the architectures with an ILP model that considers traffic grooming and other related constraints. Then, we randomly select one or more OTN switches as broken to get $\mathbf{R}^a$ with a fixed total traffic volume, and then restore the affected flows with our proposed MLR algorithm. Fig. 2 shows the simulation results.

In Fig. 2(a), we observe that *Architecture* I does not reconfigure any LCs. This is because it does not use electrical grooming but sets up a new lightpath for each flow. Hence, when failure(s) happen in the electrical layer, the flows in *Architecture* I either become unrecoverable (*i.e.*, their sources or destinations are broken) or intact (as shown in Fig. 1), which means that MLR is not needed. The same reasoning applies to the results in Fig. 2(b). When comparing *Architectures* II and III, we can see that *Architecture* III reconfigures much more LCs than *Architecture* II. Note that, the MLR in *Architecture* III does not need to reconfigure ECs since end-to-end encryption is used there. As the unit cost of reconfiguring an LC is relatively low, the MLR in *Architecture* III would prefer to groom affected flows onto existing lightpaths instead of setting up new lightpaths for them. On the other hand, since *Architecture* II grooms flows before encrypting them, it needs to reconfigure both LCs and ECs if MLR tries to groom affected flows onto existing lightpaths. However, the unit cost of reconfiguring an EC is relatively high. Hence, *Architecture* II may just set up new lightpaths to restore affected flows when the cost of reusing existing lightpaths is too high. This explains the relation between the results of *Architectures* II and III in Fig. 2(a). The analysis can also be verified with the results in Fig. 2(c), which indicate that *Architecture* II uses more LCs in total than *Architecture* III. In Fig. 2(b), *Architectures* I and III do not reconfigure any ECs in MLR because they use end-to-end encryption. In Figs. 2(c) and 2(d), we plot the total numbers of used LCs and ECs, respectively. Note that, we count the LCs/ECs used for normal traffic and MLR together here for fair comparisons. It can be seen that since *Architecture* I does not need MLR, the numbers of used LCs/ECs stay unchanged. As it uses end-to-end encryption, the MLR in *Architecture* III would not use any new ECs. Hence, in Fig. 2(d), the total number of used ECs in *Architecture* III stays unchanged too. The results on total OPEX are shown in 2(e), which indicates that with our proposed MLR algorithm, *Architecture* II is still the most cost-effective one even when MLR has to be considered. However, its advantage over *Architectures* I and III can decrease significantly when the total volume of affected traffic in MLR increases.

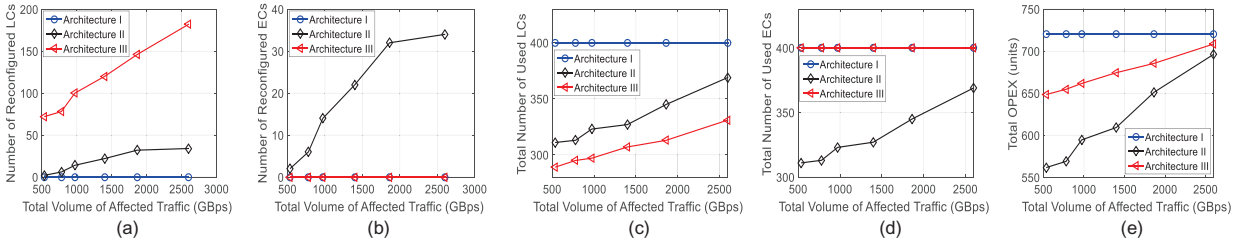


Fig. 2. Simulation results.

5. Conclusion

We studied the scenario in which an optical network with ESD can be affected by electrical layer failures, and designed an algorithm to improve the cost-effectiveness of the MLR in two architectures for such an optical network.

References

[1] "Data center connect security", *Technical White Paper*, Alcatel-Lucent, 2015.
[2] M. Medard *et al.*, *IEEE Netw.*, vol. 11, no. 3, pp. 42-48, May. 1997.
[3] J. Zhu *et al.*, *J. Lightw. Technol.*, vol. 34, no. 11, pp. 2645-2655, Jun. 2016.
[4] K. Guan *et al.*, *in Proc. of ECOC 2016*, pp. 1226-1228, Sept. 2016.
[5] R. Govindan *et al.*, *in Proc. of ACM SIGCOMM 2016*, pp. 58-72, Aug. 2016.
[6] I. Maor *et al.*, *in Proc. of ECOC 2016*, pp. 187-194, Sept. 2016.
[7] S. Liu *et al.*, *in Proc. of OFC 2017*, Paper W3I5, Mar. 2017.