Protection of Inter-ONU Connectivity in Advanced PON with Minimum Trenching Cost

Oleg Karandin[1*], Omran Ayoub[2], Domenico Napoletano[1], Francesco Musumeci[1], Massimo Tornatore[1]

[1]*Department of Electronics, Information and Bioengineering, Politecnico di Milano, Milan, Italy*
[2]*University of Applied Sciences of Southern Switzerland, Switzerland*
*Corresponding author: oleg.karandin@polimi.it

Abstract—**High-capacity and low-cost Passive Optical Network (PON) is a competitive solution for demanding applications that require low latency and high availability (e.g., 5G fronthaul). Recent proposals show that strict latency requirements can be satisfied by directly connecting Optical Network Units (ONUs) through the Remote Node, in an architecture called *Advanced PON*. To ensure high reliability of inter-ONU connections against fiber cuts, in this paper we propose two protection schemes that implement path protection and link protection in the context of advanced PONs. Our numerical results show that path protection requires (4-13)% more trenching to place spatially disjoint backup fibers compared to link protection, but might still be practical because of lower equipment complexity.**

Index Terms—**Advanced/Mesh PON, path/link protection**

I. INTRODUCTION

Passive Optical Networks (PONs) are designed to provide low-cost broadband access connectivity for residential and business clients. Latest upgrades of PON technology use multiple wavelengths carrying up to 50 Gbit/s each [1] and extend the scope of PON towards more demanding applications, e.g., 5th Generation (5G) fronthaul [2].

PON topology is a tree with an Optical Line Terminator (OLT) at the root connected to Optical Network Units (ONUs) at the leaves through a passive Remote Node (RN), which is typically a splitter/combiner. While PON's capacity is enough to provide low-cost connectivity in 5G Radio Access Networks (RAN), its point-to-multipoint architecture represents a limitation for inter-ONU communication, as it can only facilitate traffic between ONUs (e.g., hosting Radio Units (RUs) at the antenna sites) and an OLT (e.g., hosting Central Unit (CU) with computing capabilities). As strict latency requirements of novel RAN architectures and future 5G applications force data processing closer to antenna sites, PON must allow connectivity between one ONU (e.g., hosting RU) and another ONU (e.g., hosting Distributed Unit (DU), CU or even network core) with low-latency, i.e., connecting ONUs through the RN to avoid a detour through the OLT.

Novel PON architectures supporting inter-ONU connectivity have been recently introduced in literature as Advanced or Mesh PON. Ref. [3] describes different inter-ONU traffic patterns and corresponding modifications of RN architecture. Ref. [4] focuses on scalability and programmability through dynamic virtual PON slicing for inter-ONU connectivity.

From a survivability perspective, protection against device failures and fiber cuts has been so far investigated and standardized only for PONs supporting traditional OLT-ONU communications. Standard [5] defines four protection schemes, namely, type A, B, C and D, that duplicate OLT and/or RN and/or fibers connecting OLT to RN and/or RN to ONUs. However, to the best of our knowledge, protection of inter-ONU connectivity has not been investigated before, while
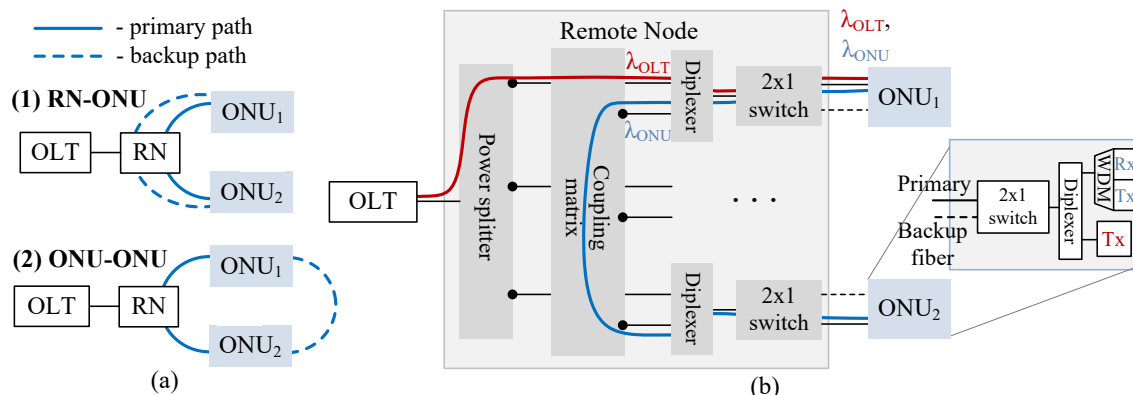

Fig. 1: (a) Proposed protection schemes for inter-ONU connectivity in PON. In (1) *RN-ONU* protection a backup path connects ONU$_1$ to RN and ONU$_2$ to RN. In (2) *ONU-ONU* protection a backup path directly connects ONU$_1$ and ONU$_2$. (b) Remote Node Architecture in Advanced PON with *RN-ONU* protection. A coupling matrix interconnects ONUs, while diplexers filter inter-ONU and OLT-ONU traffic carried at different wavelengths. Switches choose between primary and backup fibers, and are not needed in case of *ONU-ONU* protection.

it is a critical design component to satisfy high-reliability requirements of 5G fronthaul. We propose two protection schemes for inter-ONU traffic illustrated in Fig. 1a: (1) *RN-ONU protection* inspired by link protection and (2) *ONU-ONU protection* inspired by path protection.

To provide protection against fiber cuts, backup fibers must be placed in spatially disjoint trenches. Using an Integer Linear Programming (ILP) model, in this paper we compare two protection schemes numerically in terms of trenching and fiber cost and qualitatively in terms of hardware complexity. We find that *ONU-ONU* protection requires more trenching, however, for certain traffic scenarios, cost increase is small and may be potentially compensated by the lower complexity of the RN.

II. PROTECTION OF INTER-ONU CONNECTIVITY

A. RN-ONU vs. ONU-ONU Protection

We propose two protection schemes for inter-ONU connectivity (see Fig. 1a): (1) *RN-ONU protection* that installs a backup fiber from RN to each protected ONU and (2) *ONU-ONU protection* that installs a backup fiber directly between the protected ONUs. In this work we assume that i) primary path always goes through the RN (see Fig. 1a) according to the tree topology of PON, and ii) primary and backup fibers must be placed into spatially disjoint trenches to reduce the probability of them being cut simultaneously.

RN is equipped with diplexers, so that OLT-ONU traffic and inter-ONU are carried over the same fibers, but at different wavelengths (red and blue wavelengths in Fig. 1b, respectively). This makes *RN-ONU* protection compatible with the existing standards for OLT-ONU traffic protection, as the same backup fiber can protect both inter-ONU and OLT-ONU traffic against a fiber cut, and can potentially be connected to the duplicate RN.

In case of *ONU-ONU* protection, only primary fibers are connected to the RN, reducing the number of RN ports and eliminating the 2x1 switches that choose between primary and backup fibers in *RN-ONU* protection. However, *ONU-ONU* protection can guarantee OLT-ONU connectivity in case of a fiber cut only if primary fibers between RN and both ONUs are deployed in spatially disjoint trenches. In this case, if a primary fiber is cut, the ONU connects to the OLT through the other ONU (that should be able to act as a relay, further complicating its architecture with respect to Fig. 1b). Moreover, *ONU-ONU* protection makes inter-ONU traffic resilient to RN failures, as backup paths do not cross it, but, for the same reason, extra fibers between ONUs and duplicate RN must be deployed to protect OLT-ONU traffic against RN failure.

B. Illustrative Example

We consider two inter-ONU connectivity patterns common to Cloud-RAN. In *one-to-any*, shown in Fig. 2a, a single ONU with computing capabilities (node 1) is located at the node with the highest degree in the trenching topology and requires low-latency connectivity with all other ONUs (nodes 2, 3, 4) that host RUs. Road layout (grey lines) constrains candidate trenches that can host primary and backup fibers (in blue). We
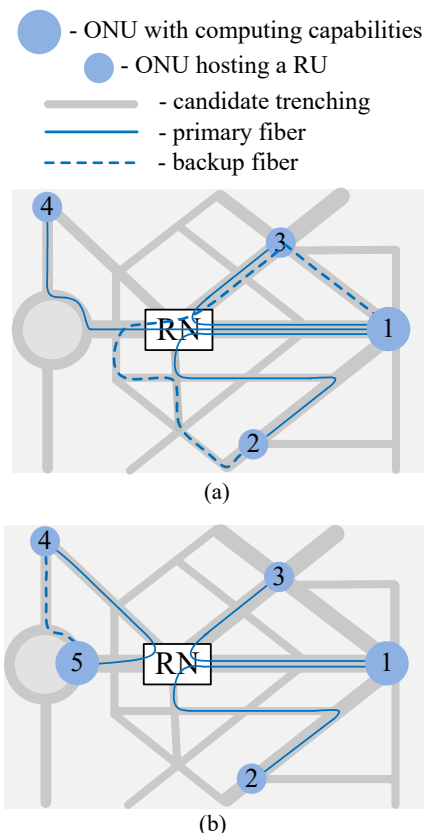

Fig. 2: Primary and backup fibers (solid and dotted blue lines) mapped over the candidate trenching topology (grey lines), defined by the road layout, considering (a) one-to-any traffic with *RN-ONU* protection of connectivity between nodes 1 and 2 and (b) few-to-any traffic with *ONU-ONU* protection of connectivity between nodes 4 and 5

assume that *RN-ONU* protection is used for traffic between nodes 1 and 2, and hence we place backup fibers (a dotted blue line) that connect node 2 to RN and RN to node 1 but are link-disjoint from the primary fibers (a solid blue line).

In *few-to-any*, illustrated in Fig. 2b, multiple ONUs with computing capabilities (nodes 1, 5) are randomly placed in the nodes, and require connectivity with their neighboring ONUs that host RUs (nodes 2, 3, 4), so that each ONU is connected to only one computing node. We assume that *ONU-ONU* protection is used for traffic between nodes 4 and 5, and place a fiber (a dotted blue line) that directly connects node 4 to 5 and is link-disjoint from the primary fibers that connect 4 to RN and RN to 5.

III. INTEGER LINEAR PROGRAMMING MODEL

To evaluate the cost of the proposed protection schemes, we formulate an ILP. The optimization problem solved by the ILP can be summarized as: **Given** candidate trenching topology *G(N,E)*, set of inter-ONU demands *P*, set of inter-ONU demands that require protection *B*, **Find** the mapping of the primary and backup fibers on the candidate trenches, with the **Objective** of minimizing the total trenching and fiber cost. The main **Constraints** are link-disjointness of primary

TABLE I: Parameters and sets of the ILP models

Set or parameter	Description
G(N,E)	Undirected graph representing candidate trenching topology, with a set of nodes N and set of candidate links-trenches E
A	Set of directed links-trenches
l_{ij}	Length of link $(i,j) \in A$
RN	Index of the Remote Node
P	Set of source-destination node pairs (s,d) of primary fibers with $s = RN$ and $d \in N, d \neq RN$
B_{RN-ONU}	Set of source-destination node pairs (s,d) of backup fibers with $s = RN$ and $d \in N, d \neq RN$
$B_{ONU-ONU}$	Set of source-destination node pairs (s,d) of backup fibers with $s \in N, s \neq RN$ and $d \in N, d \neq RN$
d	Maximum length of RN-ONU or ONU-ONU fiber
C_T, C_F	Per-km cost of trenching and fiber in cost units

TABLE II: Variables of the ILP models

Variable	Description
y_{ij}	Binary, equal to 1 if there is a trench between node pair $(i,j) \in E$
x_{ij}^{sd}	Binary, equal to 1 if primary fiber between node pair $(s,d) \in P$ passes through trench $(i,j) \in A$
z_{ij}^{sd}	Binary, equal to 1 if backup fiber between node pair $(s,d) \in B$ passes through trench $(i,j) \in A$
t^{sd}	Binary, equal to 1 if there is a backup fiber between nodes $(s,d) \in B_{RN-ONU} \bigcup B_{ONU-ONU}$

and backup paths (additionally, of the two primary fibers, when *ONU-ONU* protection is used) and maximum path length.

We will describe the ILP models for the RN-ONU, ONU-ONU and Hybrid (any of the two protection schemes can be chosen for each protected inter-ONU demand) protection strategies.

Sets and parameters, and variables are described in Tables I and II, respectively.

Objective: We minimize the total trenching and fiber cost, using costs per km from [7]. Note that trenching cost is orders of magnitude larger than fiber cost ($C_T >> C_F$) and dominates the total cost.

$$\min C_T \times \sum_{(i,j)\in E} y_{ij}l_{ij} + C_F \times \sum_{(i,j)\in A} \sum_{(s,d)\in P} x_{ij}^{sd}l_{ij} +$$
$$C_F \times \sum_{(i,j)\in A} \sum_{(s,d)\in B} z_{ij}^{sd}l_{ij} \quad (1)$$

Sets, parameters, variables and objective function are the same for all strategies, while we distinguish the constraints.

A. RN-ONU protection

In this model $B = B_{RN-ONU}$ (see Table 1).

Solenoidality constraints guarantee that primary (Eqn. 2) and backup (Eqn. 3) fibers are continuous.

$$\sum_{(i,j)\in A} x_{ij}^{sd} - \sum_{(j,i)\in A} x_{ji}^{sd} = \left\{ \begin{array}{ll} 1 & i = s \\ -1 & i = d \\ 0 & otherwise \end{array} \right.$$
$$\forall i \in N, \ \forall (s,d) \in P \quad (2)$$

$$\sum_{(i,j)\in A} z_{ij}^{sd} - \sum_{(j,i)\in A} z_{ji}^{sd} = \left\{ \begin{array}{ll} 1 & i = s \\ -1 & i = d \\ 0 & otherwise \end{array} \right.$$
$$\forall i \in N, \ \forall (s,d) \in B \quad (3)$$

Link usage constraints guarantee that there is a trench between nodes (i,j) if there is a primary (Eqn. 4) or backup (Eqn. 5) fiber mapped on that trench. Eqn. 5 additionally makes sure that for the same source-destination node pair there is either a primary or a backup fiber placed in the same trench, but not both. Note that $s = RN$ (see Table I).

$$x_{ij}^{RNd} + x_{ji}^{RNd} \leq y_{ij} \quad \forall (i,j) \in E, \ \forall (s,d) \in P \quad (4)$$

$$x_{ij}^{RNd} + z_{ij}^{RNd} + x_{ji}^{RNd} + z_{ji}^{RNd} \leq y_{ij}$$
$$\forall (i,j) \in E, \ \forall (s,d) \in B \quad (5)$$

Fiber length constraint limits the length of the primary (Eqn. 6) or backup (Eqn. 7) fiber to guarantee sufficient power at the receiver.

$$\sum_{(i,j)\in A} x_{ij}^{sd} \times l_{ij} \leq d \quad \forall (s,d) \in P \quad (6)$$

$$\sum_{(i,j)\in A} z_{ij}^{sd} \times l_{ij} \leq d \quad \forall (s,d) \in B \quad (7)$$

B. ONU-ONU protection

In this model we assume that $B = B_{ONU-ONU}$ and substitute Eqn. 5 with Eqn. 8 to guarantee link-disjointness of the two primary fibers, and not only the primary and backup fibers, as in the RN-ONU protection scheme.

$$x_{ij}^{RNs} + x_{ij}^{RNd} + z_{ij}^{sd} + x_{ji}^{RNs} + x_{ji}^{RNd} + z_{ji}^{sd} \leq y_{ij}$$
$$\forall (i,j) \in E, \ \forall (s,d) \in B \quad (8)$$

C. Hybrid protection

In this model with assume $B = B_{RN-ONU} \bigcup B_{ONU-ONU}$ and use variable t^{sd} to determine if backup fiber is placed between nodes $(s,d) \in B$.

Hybrid constraints ensure that both backup fibers to the RN are placed if RN-ONU protection is used (Eqn. 9) and that either RN-ONU or ONU-ONU protection is used (Eqn. 10).

$$t^{RNs} = t^{RNd} \quad \forall (s,d) \in B_{ONU-ONU} \quad (9)$$
$$t^{RNs} + t^{sd} = 1 \quad \forall (s,d) \in B_{ONU-ONU} \quad (10)$$

Constraints Eqn. 11-13 ensure that backup fibers are placed only for the chosen protection type.

$$\sum_{(i,j)\in A} z_{ij}^{RNs} \leq M \cdot t^{RNs} \quad \forall (s,d) \in B_{ONU-ONU} \quad (11)$$

$$\sum_{(i,j)\in A} z_{ij}^{RNd} \leq M \cdot t^{RNd} \quad \forall (s,d) \in B_{ONU-ONU} \quad (12)$$

$$\sum_{(i,j)\in A} z_{ij}^{sd} \leq M \cdot t^{sd} \quad \forall (s,d) \in B_{ONU-ONU} \quad (13)$$
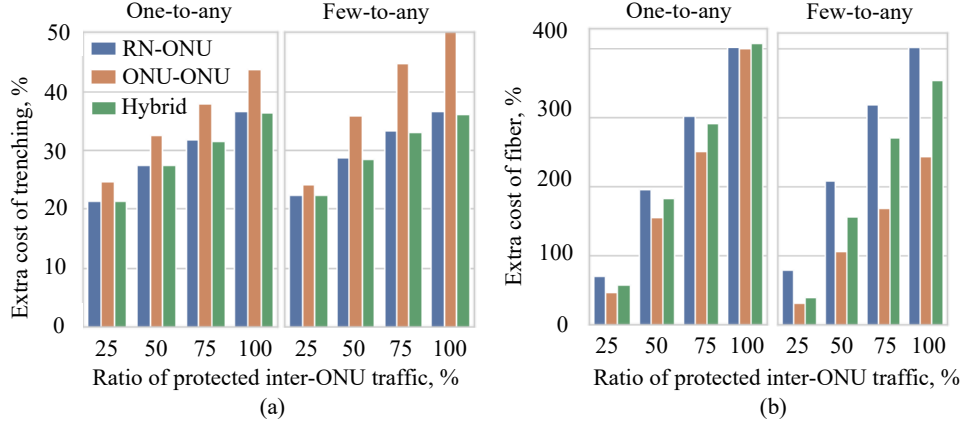
Fig. 3: Additional cost of different protection schemes w.r.t. unprotected scenario for varying ratio of protected inter-ONU traffic in terms of (a) trenching and (b) fiber

Solenoidality constraint Eqn. 2 is reused. Eqn. 3 is substituted with Eqn. 14 to enforce solenoidality for the backup fibers between RN-ONU or ONU-ONU, depending on t^{sd}.

$$\sum_{(i,j)\in A} z_{ij}^{sd} - \sum_{(j,i)\in A} z_{ji}^{sd} = \begin{cases} t^{sd} & i = s \\ -t^{sd} & i = d \\ 0 & otherwise \end{cases}$$
$$\forall i \in N, \ \forall (s,d) \in B \quad (14)$$

Link usage constraints for RN-ONU Eqn. 4 and Eqn. 5 are reused, while for ONU-ONU Eqn. 8 is substituted with Eqn. 15 and 16 to ensure that the correct link usage constraints are enforced depending on t^{sd}.

$$z_{ij}^{sd} + z_{ji}^{sd} \leq y_{ij} \quad \forall (i,j) \in E, \forall (s,d) \in B_{ONU-ONU} \quad (15)$$

$$x_{ij}^{RNs} + x_{ij}^{RNd} + z_{ij}^{sd} + x_{ji}^{RNs} + x_{ji}^{RNd} + z_{ji}^{sd} \leq 1 + t^{RNs}$$
$$\forall (i,j) \in E, \forall (s,d) \in B_{ONU-ONU} \quad (16)$$

Finally, **fiber length** constraints Eqn. 6 and 7 are reused.

IV. Case Studies and Results

To emulate the candidate trenching topology G, we generate random coordinates for 20 nodes of a RAN and find a maximal planar topology of possible trenches between the nodes using Delaunay triangulation [6]. We assign RN to a random node. We evaluate additional cost of trenching and fiber with respect to the unprotected case (set of protected demands $B = \emptyset$) for 1) RN-ONU, 2) ONU-ONU and 3) Hybrid protection scheme.

Given the same set of protected demands B, solution with RN-ONU protection is identical for one-to-any and few-to-any traffic patterns, as backup fibers connect ONUs to the RN independently on the inter-ONU connectivity, while solutions with ONU-ONU and Hybrid protection depend on the traffic pattern. We average the results over 20 random topologies and 10 random sets B of protected ONU pairs in each topology. Different types of trenching (e.g., nano, micro, mini, macro) can have different costs, however trenching always dominates

the cost of PON deployment. In this work we assume $C_T = 900$ and $C_F = 4$ [7].

A. Savings for different % of protected demands

In Fig. 3 we show the extra cost of (a) trenching and (b) fiber compared to unprotected scenario for varying ratio of protected inter-ONU traffic (i.e., 25%, 50%, 75% and 100% of randomly selected inter-ONU demands are protected), considering three protection schemes.

Fig. 3a demonstrates that RN-ONU and Hybrid protection require almost the same additional investment on trenching: (21-37)% in one-to-any and few-to-any traffic scenarios. ONU-ONU protection requires (4-13)% higher additional expenses on trenching: (25-43)% in one-to-any scenario and (25-50)% in few-to-any. This result might seem counter-intuitive (in Fig. 2a, backup path of RN-ONU must go back to the RN and appears longer than the backup path of ONU-ONU). In practice, though, this result is rational, as ONU-ONU protection requires link-disjoint trenching for the two segments of the primary path (see Section II). Hybrid scenario mostly chooses RN-ONU protection, and thus there is no extra gain in using different protection schemes in the same network. Results also show that with RN-ONU and Hybrid, protecting a larger fraction of inter-ONU connectivity (e.g., 50% instead of 25%) requires low extra cost, facilitating potential upgrades.

Fig. 3b focuses on extra cost of fiber and shows that it is lower with ONU-ONU protection, as backup fibers avoid a detour through the RN. This is especially evident in few-to-any traffic scenario, where backup fibers connect neighbouring ONUs. However, fiber cost has little effect on total cost, which is dominated by trenching.

B. Savings for different trenching topology meshedness

In Fig. 4a we show the extra cost of trenching compared to unprotected scenario for different meshedness of the candidate trenching topology, considering the three protection schemes and 100% of protected inter-ONU demands. We define graph
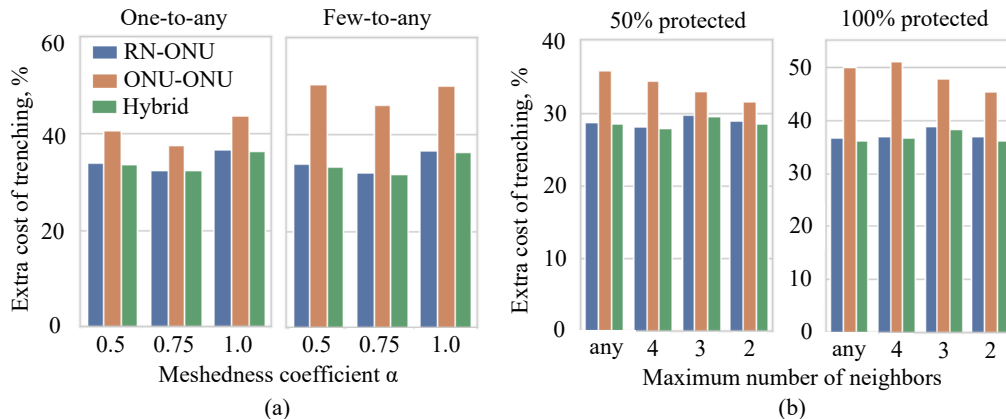
Fig. 4: Additional trenching cost of different protection schemes w.r.t. unprotected scenario for varying (a) trenching topology meshedness and (b) number of connected neighbors in few-to-any scenario

meshedness as in Eqn. 17 [6], where $|E|$ represents the number of links and $|N|$ represents the number of nodes.

$$\alpha = \frac{|E| - |N| + 1}{2|N| - 5} \qquad (17)$$

To obtain trenching topologies with different meshedness we start with maximal planar graphs generated using Delauney triangulation ($\alpha = 1$) and randomly remove edges to reduce α.

Results reported in Fig. 4a demonstrate minor variation of extra cost of trenching as α varies from 1 to 0.75 and 0.5. For instance, in one-to-any, for *RN-ONU*, extra cost of trenching ranges between 32% and 37%, and for *ONU-ONU*, the extra cost of trenching ranges between 38% and 42%. This is because the number of candidate paths decreases with the decreasing meshedness, trenching cost of both the protected and unprotected scenarios increases, and the extra cost in % remains almost constant across all scenarios. Results also show that the cost advantage of *RN-ONU* protection over the *ONU-ONU* protection does not change with the topology meshedness.

C. Savings for different number of neighboring nodes in few-to-any traffic scenario

In Fig. 4b we show the extra cost of trenching compared to unprotected scenario varying maximum number of ONUs that can be connected to the ONU with computing capabilities in few-to-any scenario (see Section II), considering three protection schemes and 50% or 100% of protected inter-ONU demands. Results show that, for both 50% and 100% of protected inter-ONU demands, extra cost remains almost constant with *RN-ONU* and *Hybrid* protection (around 30% for 50% protection, and 35% for 100% protection). This is expected, as backup fibers connect ONUs to the RN independently on the specific inter-ONU connectivity. Differently, extra cost of *ONU-ONU* protection gradually decreases.

V. CONCLUSION

We introduced and compared three protection schemes for inter-ONU connectivity in PON, *ONU-ONU* where a backup path directly connects ONUs, *RN-ONU* where a backup path connects ONU and RN, and a hybrid scheme, in terms of extra trenching and fiber cost (with respect to unprotected scenario). We model each of the protection schemes as an Integer Linear Program. We perform evaluations varying traffic patterns in Cloud-RAN and the percentage of protected inter-ONU traffic. Results demonstrated that *ONU-ONU* protection requires (4-13)% more trenching, but, in certain scenarios, the cost increase is relatively small and can be potentially tolerated because of lower hardware complexity of the RN with respect to *RN-ONU* protection. In future work we will analyze cost of protection of both OLT-ONU and inter-ONU traffic.

VI. ACKNOWLEDGMENT

REFERENCES

[1] ITU-T Recommendation G.9804.1. Higher speed passive optical networks - Requirements (2019)

[2] J. S. Wey, Y. Luo and T. Pfeiffer, "5G Wireless Transport in a PON Context: An Overview," in IEEE Communications Standards Magazine, vol. 4, no. 1, pp. 50-56, Mar. 2020

[3] T. Pfeiffer, P. Dom, S. Bidkar, F. Fredricx, K. Christodoulopoulos and R. Bonk, "PON going beyond FTTH," in IEEE/OSA Journal of Optical Communications and Networking, vol. 14, no. 1, pp. A31-A40, Jan. 2022

[4] S. Das, F. Slyne and M. Ruffini, "Optimal Slicing of Virtualized Passive Optical Networks to Support Dense Deployment of Cloud-RAN and Multi-Access Edge Computing," in IEEE Network, vol. 36, no. 2, pp. 131-138, March/April 2022

[5] ITU-T G-series Recommendations – Supplement 51. Passive optical network protection considerations (2017)

[6] M. de Berg, O. Cheong, M. J. van Kreveld, M. Overmars: Computational geometry: algorithms and applications, 3rd Edition. Springer 2008

[7] M. Mozhgan, J. Chen, L. Wosinska, A. Dixit, B. Lannoo, D. Colle, C. Mas Machuca, "Toward reliable hybrid WDM/TDM passive optical networks," in IEEE Communications Magazine, vol. 52, no. 2, pp. S14-S23, Feb. 2014