Deployment Strategies for Protected Long-Reach PON

Marco Ruffini, Deepak Mehta, Barry O'Sullivan, Luis Quesada, Linda Doyle, David B. Payne

***Abstract*—The mass deployment of fibre access networks is probably the most important network upgrade strategy for operators over the coming decade. Next generation networks, and in particular the Long-Reach Passive Optical Network (LR-PON) solution, aim to increase long term economic viability and sustainability of Fibre-To-The-Premises (FTTP) deployment. The LR-PON solution achieves this by minimising the number of nodes and the amount of electronic equipment required within the network. Since a LR-PON replaces the metro backhaul network, which is usually a protected part of the network, protecting the long reach part of LR-PON network against failures becomes a critical issue that needs to be taken into account. In this paper we introduce a novel protection mechanism that, by spreading the load generated by a node failure over the network, can significantly reduce the overall protection capacity required. We then present a practical FTTP deployment scenario based on our protected LR-PON architecture for a European country. The problem is modeled using Integer Linear Programming and the optimisation results, obtained using a real dataset provided by a national operator, show that a small number of Metro/Core nodes can provide protected connection to FTTP users. By applying a detailed cost model to the outcome of the optimisation we are able to show that our LR-PON deployment strategy that minimises the overall protection capacity, rather than just minimising fibre distances in the LR-PON, can significantly reduce costs.**

***Index Terms*—Long-Reach passive optical networks, network protection and resiliency, network optimization, cost analysis.**

I. Introduction

Over the past decade Internet traffic has grown exponentially, at a compound annual growth rate (CAGR) of about 75% [1]. Growth over the last decade has been a combination of a growth in the user base and a growth in user application and usage time, prompted by a multitude of new online content sharing applications such as Facebook, YouTube and many others. Growth in the user base in the developed countries is now beginning to saturate so that future growth will be driven by adoption of high speed access technologies such as FTTP and the higher bandwidth services these technologies can support. In particular Internet video applications, including delivery of High Definition (HD) and 3D video, show predicted yearly growth rate of 47%. Data rates for HD video applications run in excess of 10 Mbps per channel. These effects mean that future growth could also be of a similar order with CAGR projections showing ranges from about 15% to 60%, depending on the rate of FTTP deployment and take up [1],[2]. In addition, in order to deliver satisfactory Quality of Experience (QoE), especially for real-time services such as thin client computing (Google Chrome notebook is a recent example), delivering high peak data rates becomes increasingly important. Most techniques based on Digital Subscriber Line (generally know as x-DSL) struggle to provide peak bandwidth in excess of 20-30 Mbps. VDSL (Very-high-bit-rate-DSL) is capable of 50 Mbps, but it can only cover short distances (up to 300m) and is asymmetric. It is usually deployed as a hybrid copper-fibre access solution, in a Fibre-To-The-Curb (FTTC) installation. FTTP on the other hand is the only solution capable of providing the scalable access bandwidth required for the foreseeable future. Indeed the number of access fibre installations has grown exponentially in a number of countries (e.g., Japan, South Korea, the USA) over the past few years, a trend which could dominate over the next decade and become the dominant driver for network bandwidth growth.

Passive Optical Networks (PONs) are now deployed as an accepted solution for Fibre-To-The-Home (FTTH), by virtue of the ability to share equipment and fibre among a number of customers and thereby reduce costs. However the huge bandwidth capability in the access will strain the total network viability as metro and core networks will need to be upgraded to support the bandwidth demand, but with little return on investment. This problem has stimulated next generation PON investigations and among these the Long-Reach PON (LR-PON) is gaining interest as an economically viable solution. Initial ideas of optical access networks with long reach and high split date as far back as 1990 [3]. Such ideas were further elaborated over the next decade by a few research institutions, where extensions to the basic PON concepts paved the way for SuperPON [4], [5]. It's only over the past few years though that this idea has gained much popularity as Long-Reach PON. One reason for increasing interest in LR-PON is that long-reach and high-split systems have recently been demonstrated [6], [7] using relatively inexpensive devices. Two key benefits arising from LR-PON deployment are: first, by extending the optical reach to about 100 km, the number of network nodes can be reduced by as much as two orders of magnitude, eliminating electronic equipment for traffic aggregation, routing and switching at most of the local exchanges and thereby reducing both cost and energy consumption. Second, by increasing the maximum number of customers per PON from 32 to about 500 or even 1000, it increases equipment and fibre sharing, further reducing Capital Expenditures (CapEx) and thus the time to positive cash flow [8]. Current experiments [6] focus on single channel 10Gbps systems, although it is envisaged that in the future higher data rates and multi-wavelength system will be developed (hybrid WDM-TDM LR-PON).

Much of the research work on LR-PON (see [9] for an overview) has focused on challenges at the physical layer, such as suitable optical amplification for the bursty upstream traffic [10], [11], low-cost transmitters for the Optical Network Unit (ONU) [12], and high-speed burst-mode receiver at the Optical Line Terminal (OLT) [13], [14]. Additional noteworthy work was carried out on improvements to the Dynamic Bandwidth Assignment (DBA) mechanism, through multi-thread polling [15].

The work we present in this paper focuses on LR-PON

M. Ruffini, L. Doyle and D. B. Payne are with CTVR the telecommunications research centre, University of Dublin, Trinity College, Ireland (e-mail: marco.ruffini@tcd.ie).

D. Mehta, B. O'Sullivan and L. Quesada are also with CTVR, Cork Constraint Computation Centre, University College Cork, Ireland (e-mail: b.osullivan@cs.ucc.ie)

protection strategies. Although protection in current access architectures is not usually provided, with the exception of larger business customers, it becomes a relevant issue in LR-PON, because, by connecting the user premises directly to the Metro/Core (MC) node, it replaces the backhaul or metro transmission network, which usually offers protection paths to the metro or outer core nodes. A fault in the long distance part of a LR-PON or OLT can affect 500-1000 customers, while a cable cut can affect tens of thousands. However little research work has so far been carried out in LR-PON resiliency (which we discuss in the next section).

This paper brings two main contributions. First we propose the design of a novel protection mechanism that aims at reducing the over-provisioning of IP routing resources dedicated to network protection, while ensuring resiliency against large scale failures (initial results were reported in [16]). Second, we propose a novel deployment strategy for the layout of LR-PONs, which, in synergy with the protection mechanism introduced, minimises the IP routing resources used for protection. Our study, carried out using real data provided by the major Irish telecom operator, shows that significant CapEx savings can be achieved, compared to a dual-parenting protection scheme obtained by doubling IP routing equipment. In the next section we provide an overview on related work by standardization bodies and research groups.

II. Related work on GPON protection and its LR-PON evolution

Protection mechanisms have been designed into PON standards. However their implementation is an optional feature, as indicated for example in the ITU-T Gigabit Passive Optical Network (GPON) standard: “protection shall be considered as an optional mechanism because its implementation depends on the realization of economical systems” [17]. The cost incurred in providing protection for an access network can in fact be considerable. It includes, among other equipment, provision for backup optical fibre paths, OLT cards, additional IP capacity, plus it increases complexity at the network control and management layers. The benefits include a fast service restoration after a failure occurs, which for a non-protected system could take as long as the time required to physically repair the failure. The GPON standard defines multiple protection options to offer different degrees of resilience. A first distinction is between a “duplex” and a “dual-parented” (or equivalently “dual-homed”) system. In the former, the primary and backup feeder fibre, which connects OLT to first-stage split, are both terminated in the same node, while in the dual-parenting case (reported in Fig. 1 for a LR-PON scenario), the primary and backup OLTs are geographically separated. Among the two solutions the second provides a higher level of resiliency because it increases the network reliability against local disasters, such as fires, earthquakes or floods. In addition, the backup fibre ideally needs to follow a different geographical route in order to provide protection against cable cut (i.e., it needs to be routed over a different Shared Risk Link Group - SRLG), thus in this case any cost saving in locating the two OLTs at the same physical location are minimal.

A second distinction among protection options is between an “OLT-only” and a “full” protection system. The former only duplicates the feeder fibre (shown in Fig. 1 for a LR-PON scenario), while the latter also duplicates the Optical Distribution Network (ODN), i.e. the part that goes from the splitter to the ONU (duplicating also the line terminator within the ONU). Although the second option provides higher resiliency, because it protects against failure in the access portion of the network that is closer to the user, it is effectively a full duplication of the network and is usually considered too expensive for general deployment and operators would only provide this solution for larger business customers who specifically request full geographic separation for the protection path and are willing to bear the extra cost.

Overall, protection mechanisms for LR-PON follow similar general guidelines. However a number of additional issues arise. The longer reach of the LR-PON enables replacement of the metro/aggregation network. The long lengths of fibre cable that can be present in this feeder part of the LR-PON network have significantly increased probability of service interruption from cable dig-ups. As each LR-PON could be supporting about 500 or even 1000 customers and the fibre cable could be feeding several LR-PON systems, a cable cut could affect thousands of customers. Also the “metro network” fibre would normally have been part of a resilient network, e.g., SDH ring systems. A catastrophic failure at a Metro/Core (MC) node could bring down all the PONs terminated by the node (e.g., potentially hundreds of thousand of customers), for a period of time that, depending on the severity of the accident, could be as long as several weeks. Although such large-scale failures are rare, it is recognized [18] that the catastrophic effects they would cause would not be tolerable, therefore its risk cannot be neglected.

Although the active electronic switching and transmission equipment previously housed in the local exchange site has been eliminated by the LR-PON solution, the high loss of the extended reach and higher number of splits needs to be counteracted by using optical amplifiers. Thus the LR-PON is not strictly passive between the ONU in the customer premises and the OLT in the MC node. The optical network active elements (i.e., the optical amplifiers, signaling and management electronics, and power supplies) require additional protection, because their typical time between failures (TBF) is shorter compared to the passive elements. In [18] the authors carry out a detailed analysis of protected amplified GPON, considering equipment and fibre duplication at multiple points: at the fibre feeder through dual-parenting, at the first splitter for the optical amplifiers, and at additional splitting stages up to the customer ONU. Their results show that the best compromise between availability and deployment costs is achieved by protecting the fibre feeder through a dual-homing solution (also protecting the optical amplifier). Additional protection equipment does increase network availability, but only marginally, while costs soar disproportionately. It is realistic to consider a scenario where most users (residential and small business) are protected by dual-homing the fibre feeder, while more resilient links, including for example a secondary diverse route to the premises terminated on a backup ONU, are employed for demanding business users.

Although most LR-PON solutions are based on a “tree and branch” topology, a few solutions [19], [20] were proposed that consider ring topology for aggregating traffic from a number of splitters towards the OLT. The main advantage of using ring architectures, from a resiliency point of view, is that they can inherit the fast protection switching mecha-

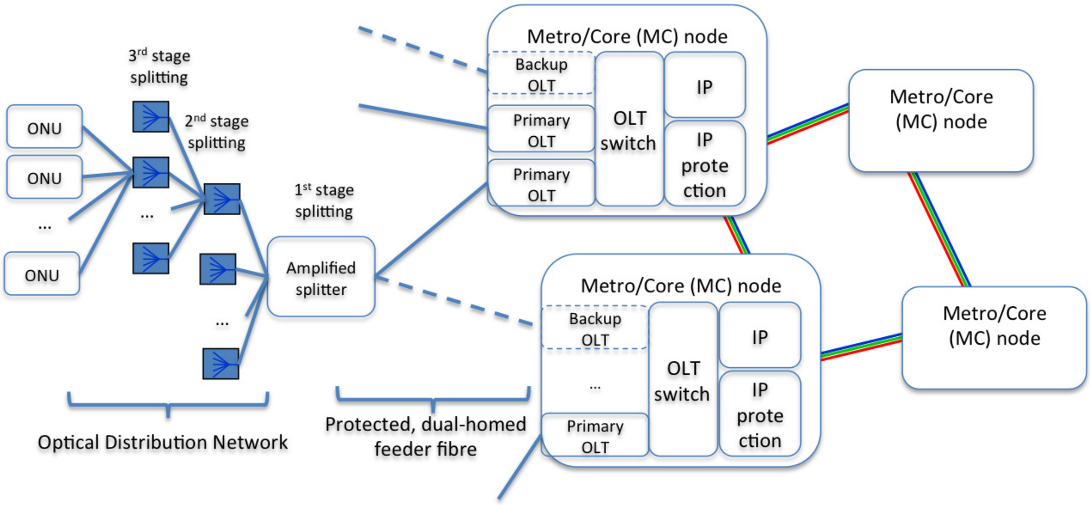


Fig. 1: Example of a 3-stage LR-PON deployment, showing both metro/access and core/backbone networks

nism from Synchronous Optical Network / Synchronous Digital Hierarchy (Sonet/SDH) technology. One of the drawbacks however is that it requires the use of add-drop nodes, which depending on the technology used (i.e., whether they are electronic or optical add-drops), can increase costs, power consumption and optical power budget. In addition, since a large proportion of the duct network in developed countries was laid before the appearance of Sonet/SDH ring network topology, ring solutions do not provide short distance paths between nodes and are usually much longer than the equivalent "point to point" paths required for the tree and branch LR-PON solution.

In this work we focus on protecting the fibre feeder with dual-homing and the optical amplifier at the first-stage split. Figure 1 shows the case of an OLT-only dual-parented system. The 3-stage PON splitting is designed to reuse current access network ducting: the first splitting stage, which also houses the optical amplifiers for the LR-PON, is placed at the local exchange site (preferably in the cable chamber or in a cabinet so the building can be released for alternative use), the second is at the cabinet location and the third at the distribution point. Special cases could however deviate from this situation, and employ either additional or fewer stages. While the protection cost on the OLT side of the amplified splitter is shared among all the customers of a PON (i.e., up to 32 for a GPON system and up to 1000 for LR-PON), the cost incurred in protecting the ONU side becomes progressively less cost-effective as we pass from the first-stage towards the third, where sharing is progressively reduced, and will only be economically viable for a subset of business customers that require high resiliency (and can incur the additional cost).

In the following sections we describe our LR-PON protection and deployment strategies, based on a network design that considers protection associated costs at the outset. We consider two main cost contributions: fibre deployment and general PON equipment costs on the one hand, and working and protection costs at the IP layer [21] on the other hand. The particular focus on the IP layer is due to its high contribution to equipment costs in metro and core nodes. Traditionally the IP layer is protected with a 1+1 or 1:N scheme. In the first, the router capacity is doubled, generating an over-provisioning of 100%. Capacity doubling is achieved by employing two separate routers, each operating at 50% (or less) of their full capacity, so that if one fails, the second can support the entire node load. Such routers can also be deployed on separate locations to provide additional resiliency (dual-homing). The second scheme, 1:N [22], is used for protecting IP cards, and it allows protecting N active IP cards through 1 backup card. Such scheme only offers resilience against failure of individual IP cards, while not protecting for larger failures. In this paper, we consider as worst case scenario the failure of an entire metro/core node, thus we compare the PON and IP protection schemes we propose to the 1+1 protection method.

III. Efficient sharing of protection resources

The ODN part of a LR-PON can be represented by a tree topology rooted at the 1st stage split. In the protected dual-homed configuration the root is connected to a primary OLT, which provides the service, and to a backup OLT, which takes over if a failure occurs in the primary link or at the OLT. The node hosting the primary OLT is referred to as primary metro/core (MC) node for that LR-PON, while the node hosting the backup OLT is the secondary MC node. Due to the large coverage allowed by LR-PON, primary and secondary MC nodes of exchange sites can be spaced several kms apart, thus increasing the geographic resiliency of the network. In this section we design a coverage mechanism for Long-Reach PON, originally presented in [16], that reduces the over-provisioning needed for protection equipment, by distributing the additional load generated by a node failure over the network.

A. *Territory coverage through a honeycomb structure*

Each MC node offers fibre access to a geographical area identified by a circle centered at the node, with radius equal to the optical reach divided by a routing factor. The routing factor accounts for the fact that the length of fibre needed to connect two network points is larger than their Euclidean distance, because fibre paths tend to follow road layouts. In Ireland, considering a value of 1.4 for the routing factor and 100 km for the optical reach, each MC node covers an area with radius equal to 71.5 km. Protection is provided by overlapping coverage areas of adjacent MC nodes. If we approximate each circle with the inscribed hexagon, a country can be covered with a honeycomb structure, similar to that used for cellular topologies. Figure 2 shows a coverage example for the Republic of Ireland, where basic unprotected coverage can be achieved with 9 nodes. Protection could be applied to this scheme by simply duplicating the equipment at each node (i.e., using duplex rather than dual-parented protection, as mentioned in section II). Graphically, this corresponds to overlapping each coverage circle with an additional circle (i.e., using 18 nodes), thus duplicating the feeder fibre, the OLTs and routing equipment, leading to an over-provisioning ratio of 100%.

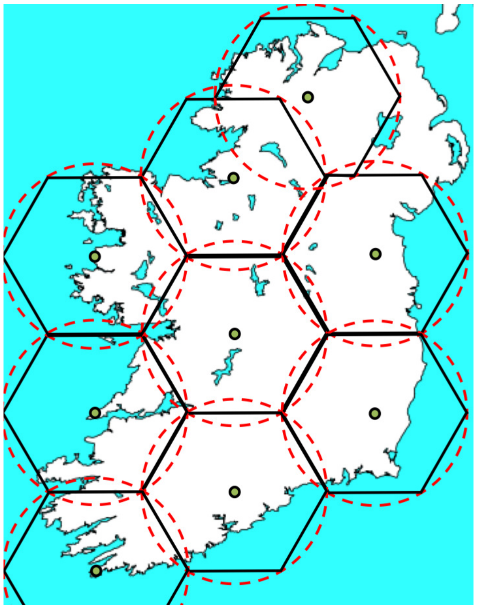


Fig. 2: Example of a LR-PON coverage plan for Ireland

The alternative strategy we propose is that each area is protected by overlapping the minimum number of non concentric circles. This is achieved in Fig. 3 by centring three additional circles (centred at nodes B, C and D) at the edge of the coverage area of node A. We have calculated that such coverage also requires 18 nodes in order to provide resilient coverage for Ireland. Although our mechanism also duplicates the feeder fibre and the number of OLTs for protection purposes, due to the partial overlap of the MC coverage areas, the over-provisioning of IP routing equipment for protection is notably reduced compared to 1+1 dual parenting. This statement can be explained as follows.

Looking at Fig. 3, each node offers primary coverage to the PONs that are closer to it than to any other adjacent node. These areas are known as “Voronoi cells” [23] in the Euclidean space and the MC nodes are located in the “Voronoi sites”. In the figure these are the equilateral triangles covered with triangle shades, with circumcentre at A, B, C and D. In addition, since each node can physically cover an area as large as the hexagonal cell (drawn in red dotted line), it can provide protection for those areas within the hexagon but external to the triangle. For example, in the figure, B1, C1 and D1 represent part of the areas primarily covered by nodes B, C and D, for which A provides protection. Due to the symmetry of the construction, both primary (i.e., the larger equilateral triangles) and protected areas (i.e., the sum of the three smaller triangles, for example B1, C1, and D1), for each node, are equal to half the area of the hexagonal cell. Since we consider as worst-case scenario the total failure of one single node, the advantage of this triple coverage is that if any node, say A, fails, its load (which here is assumed to be proportional to the area covered by the triangle centred at A) can be equally shared among the adjacent nodes, B, C and D, which protect, respectively, sectors A1, A2 and A3. In the simple case of equally distributed load and coverage in the network the maximum amount of over-provisioning for protection capacity that *each node* needs to contribute for is equal to about 33% (i.e., one third) of the normal working load. This is a major improvement over the 100% over-provisioning required by the 1+1 protection mechanism. In the next section we introduce an extension we have developed to the triple-coverage mechanism that allows sharing the protection load over the entire network, so that the lower bound on the over-provisioning resources required for protection at each node can be reduced well below the 33% value.

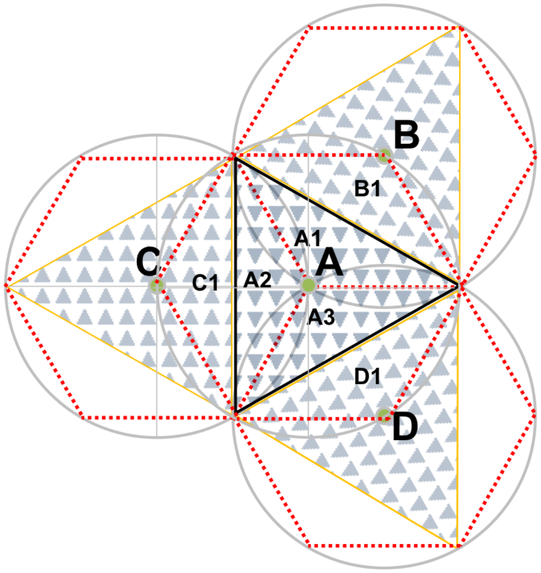


Fig. 3: Coverage protection by overlapping three non-concentric areas

There are issues that can arise from our triple-coverage strategy. The first is that there are border effects, in the sense that the most external areas of the structure only provide primary coverage. This means that some additional nodes might be required to provide protection for such areas, which would increase the required over-provisioning above the ideal value of 33%. The effect is more evident for smaller geographies, where the number of border nodes is large compared to the overall number of nodes. Such effects also depend on the geography of the country, and for example are negligible for Ireland because the unprotected areas lie either over the sea, or else over sparsely populated parts of the territory. In cases where edge effects might constitute an issue, the situation can be improved by tuning the distances within the honeycomb structure, by positioning additional nodes, or, where possible, by increasing the optical reach of the network at selected spots.

B. Sharing of protection resources over the network

We have elaborated an extension to the previously introduced protection method that further reduces the IP over-provisioned capacity required at a node to handle the off loaded traffic from an adjacent node failure. Considering Fig. 4, if node A fails, nodes B, C and D will accept the traffic from protected sectors A1, A2 and A3 respectively (shaded rectangles). We have seen that if the load is equally distributed among the nodes this implies an additional IP protection capacity of 33% at each node. However these nodes can, in turn, pass on to their adjacent nodes part of their primary traffic, thus reducing the amount of IP traffic they carry. Node C, for example, which is protecting sector A2, simulates partial failures in sectors Cp2 and Cp3 (shaded circles), which will be protected by nodes E and F. Therefore, although C needs to provide IP protection resources for covering A2, it can offload the resources that were needed to cover Cp2 and Cp3. If this process is iterated, each node needs to protect (and therefore be over-provisioned for) a percentage of their normal working load, which is smaller than 33%.

It should be stressed that the MC nodes do not pass on the traffic from the original failed node. Rather they pass on some of their working traffic to the adjacent nodes via the protection mechanism. What is occurring is a pre-emptive re-distribution of traffic in response to a major network failure. This method significantly reduces the IP routing resources required for protection purposes at each node, leading to significant cost savings.

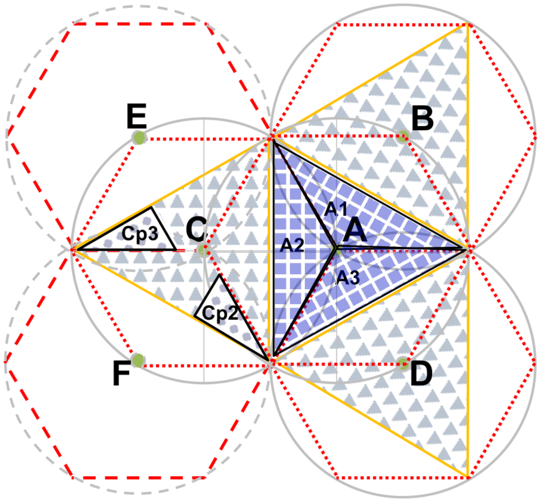


Fig. 4: Operation of our load spreading strategy

C. Optimization model for load sharing

The load sharing algorithm we have developed allows sharing the IP load coming from a network failure over the entire network, so that overall protection capacity needed at the IP layer is sensibly reduced. We consider as a worst case scenario the total failure of any one LR-PON MC node in the network (which could cover an overall area of about $16,000km^2$). In this study we focus on the IP layer, which represents one of the highest equipment costs in the MC node. Additional costs reduction by sharing other protection equipment such as OLT cards will be addressed in future work.

We have modelled our load sharing method as an Integer Linear Programming (ILP) problem, and solved it using the CPLEX optimizer [24]. The aim is to allocate protection load and load transfer among the nodes, so that over-provisioning of IP capacity for protection purposes is minimised, while ensuring that any total node failure can be protected. The topology of a LR-PON can be modelled as a graph, $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is a set of nodes and $\mathcal{E}$ is a set of directed edges. An edge from node i to node j, $\langle i, j \rangle$, represents that i can pass its partial/full load to j, if required. The customers that are passed from i to j are assumed to be covered by both i and j such that i is their primary node and j is their secondary node. The ILP formulation of the problem, comprising constants, variables, constraints and objective function, is described below.

Constants:

- Q_i: initial load for MC node i
- U_{ij} maximum load that node i can pass to neighbor node j
- $\mathtt{SP}_{ij}$: shortest path (expressed in number of hops) between any nodes i and j
- h: maximum distance from the failed node (expressed in number of hops) over which the protection load is shared

Variables:

- T_{ijk}: load that is passed from node i to j when k fails
- I_{ik}: sum of incoming loads that i receives from its neighbours when k fails
- O_{ik}: sum of outgoing loads that i passes to its neighbours when k fails
- F_{ik}: final load of i that includes the over-provision capacity that is required when k fails
- M_i: for each node i, this is the maximum among the final loads over all possible individual node failures

Constraints:

- $I_{ik} = \sum_{\langle j,i \rangle \in \mathcal{E}} T_{jik}$: the incoming load of i when k fails is equal to the sum of loads passed from each neighbor j
- $O_{ik} = \sum_{\langle i,j \rangle \in \mathcal{E}} T_{ijk}$: the outgoing load of i when k fails is equal to the sum of the loads passed to each neighbor j
- $I_{kk} = 0$: when k fails, its incoming load is zero
- $O_{kk} = Q_k$: when k fails its outgoing load is equal to its initial load
- if $\mathtt{SP}_{ki} > h$ then $I_{ik} = 0$: limits the load sharing to nodes that are maximum h hops away from the failed node k
- $F_{ik} = Q_i + I_{ik} - O_{ik}$: when k fails, the final load of i is the sum of its initial load and the required over-provisioning capacity
- $M_i \geq F_{ik}$: the load capacity of a node i has to be greater than or equal to the maximum of final loads over all possible node failures k

Objective:

- minimise $\sum_{i \in \mathcal{V}} M_i - Q_i$, ie. the total IP protection capacity required over all MC nodes. It is also desirable to minimize the number of customers that are affected. Therefore, we use $\sum_{i \in \mathcal{V}} \alpha \times (M_i - Q_i) + \sum_{\forall i,j,k \in \mathcal{V}} T_{ijk}$ as the objective, where α is any constant that is greater than $\sum_{\forall i,j,k \in V} T_{ijk}$.

D. Results for simulated networks

We have tested the load spreading algorithm described above on a network topology where each node (except those at the boundaries) has degree three (such topology is represented on the left side of Fig. 7). We have repeated the experiment for networks of different sizes (with 20, 50 and

100 nodes). For the IP traffic loads we have considered both random uniform distributions and preferential distributions (which is more suitable to characterise the skewed load distribution typical of Ireland [25]). The results we provide are averaged over ten different load scenarios. The plot in Fig.5 shows the percentage of IP protection capacity needed to protect for total failure of any one node. We have assume three different load scenarios: uniform, preferential and equal load distribution (which although unrealistic, can be considered a lower bound). The value in the x-axis is a function of the number of nodes sharing such load. It represents the number of hops away from the failed node, where the load can be shared. So a value of one indicates that the load is only shared among the first-hop, or direct neighbours of the failed node. A value of two indicates that the load is shared among all nodes that are up to two hops away from the failure, and so on. The obvious observation we make from the graph is that the larger the portion of the network sharing the load, the lower the overall protection capacity needed. In addition larger networks allow better load sharing. It is also interesting to notice that for the uniform and preferential distributions the curves tend to reach their asymptotic minimum value for a number of hops which is significantly less than the network diameter, which is 7, 11 and 16 respectively for the topologies with 20, 50 and 100 nodes. Therefore there is no need to share the load among all nodes to reach the minimum protection capacity requirement. By comparing the results for the different load distributions we can see that the load sharing ability is reduced the more skewed is the traffic distribution. Higher load inequality in fact poses stronger constraints on the amount of load that can be passed among neighbours, reducing the ability to share the load from a failed node over the whole network. Note that for simple 1+1 protection the over-provisioning would be 100%.

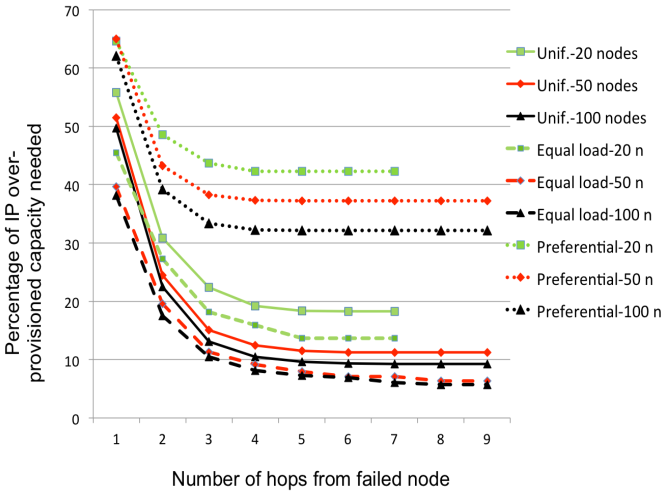


Fig. 5: Percentage of IP protection capacity, in relation to the primary IP load, for simulated networks of different sizes

The drawback of larger load sharing is that more customers not directly affected by the node failure become affected by the protection process. Load sharing operations are implemented through artificial OLT failures that might cause temporary disruption to customers. The extent of such disruption will depend on the switching time of the protection mechanism and would be unnoticeable if switching operations were below 50 ms. In [21] it was shown that theoretically at the IP layer protection switching could be reduced to less than 50 ms, via a method based on database synchronisation in IP routers. In [26] the authors carry out practical protection switching experiments, obtaining an average value of 26 seconds for full restoration of Ethernet services over a dual-hoed GPON. The authors however recognize that this could be reduced to values below 500 ms, if the switching mechanism was optimized and implemented in hardware.

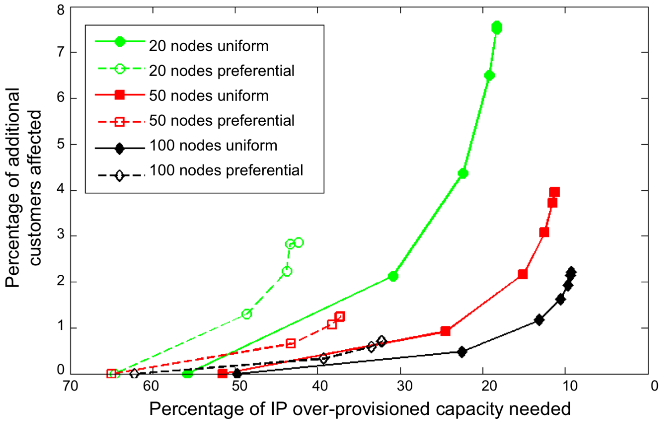
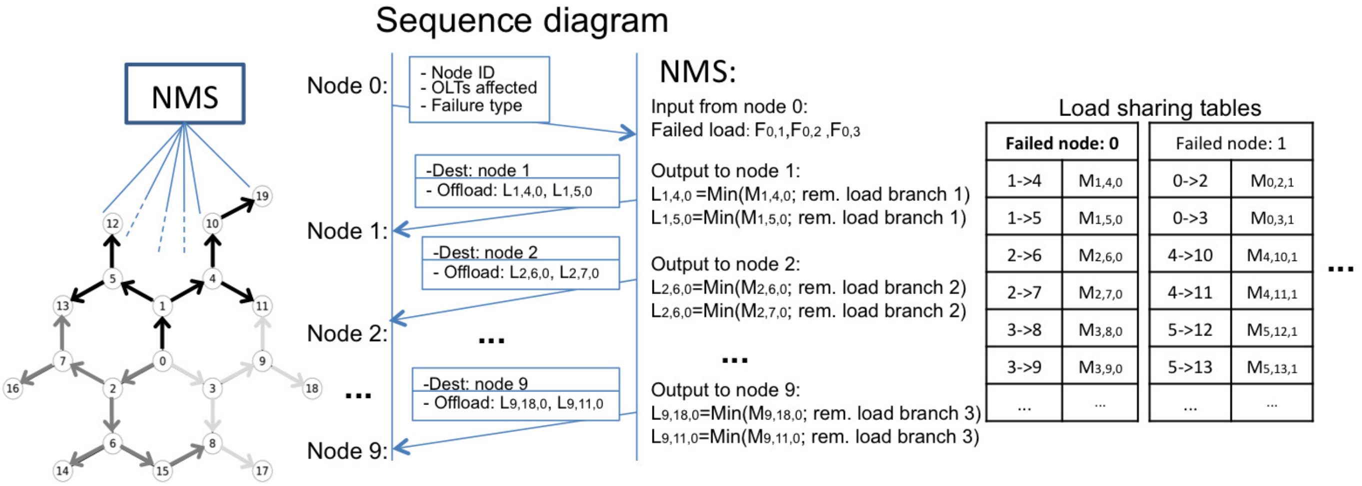


Fig. 6: Additional customers affected by a total node failure because of the load sharing mechanism, versus overall IP over-provisioning required

We have analyzed, in Fig. 6, the average percentage of additional customers affected by a failure versus the average IP over-provisioning capacity needed in the network, for networks of different sizes. The results show that the percentage of customers affected decreases as the network size increases, while it increases as we reduce the IP over-provisioning by sharing the load between more nodes. The plots show that when considering uniform traffic distribution, for a 100 node network the proposed mechanism can reduce the over-provisioning requirement to as little as 10% while only affecting 2% additional customers. For the preferential distribution case, the minimum over-provisioning requirement is noticeably over 30% because the skewed distribution leads to a less effective load sharing. This however also reduces the percentage of customers affected by the process (to about 0.8%). Such results suggest that even if the protection switching time is greater than 50 ms user disruption could be tolerated if the IP protection savings are sufficient.

E. System implementation

In this section we briefly introduce how the load-sharing mechanism we propose can be implemented through centralized operations. Load sharing tables, which store information on the amount of traffic that each node should offload towards its neighbours once a failure occurs, are calculated off-line by the Network Management System (NMS) using the ILP model introduced in section III-C. When a failure occurs (Fig. 7), the node affected raises an alarm to the NMS, which, after consulting the sharing tables, sends instruction to each node indicating the amount of traffic load that should be offloaded to downstream neighbours (where downstream


Sequence diagram
NMS
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
Node 0:
- Node ID
- OLTs affected
- Failure type
Node 1:
-Dest: node 1
- Offload: L1,4,0, L1,5,0
Node 2:
-Dest: node 2
- Offload: L2,6,0, L2,7,0
...
-Dest: node 9
- Offload: L9,18,0, L9,11,0
Node 9:
NMS:
Input from node 0:
Failed load: F0,1,F0,2 ,F0,3
Output to node 1:
L1,4,0 =Min(M1,4,0; rem. load branch 1)
L1,5,0=Min(M1,5,0; rem. load branch 1)
Output to node 2:
L2,6,0=Min(M2,6,0; rem. load branch 2)
L2,6,0=Min(M2,7,0; rem. load branch 2)
...
Output to node 9:
L9,18,0=Min(M9,18,0; rem. load branch 3)
L9,11,0=Min(M9,11,0; rem. load branch 3)
Load sharing tables
...

Failed node: 0	
1->4	$M_{1,4,0}$
1->5	$M_{1,5,0}$
2->6	$M_{2,6,0}$
2->7	$M_{2,7,0}$
3->8	$M_{3,8,0}$
3->9	$M_{3,9,0}$
...	...

Failed node: 1	
0->2	$M_{0,2,1}$
0->3	$M_{0,3,1}$
4->10	$M_{4,10,1}$
4->11	$M_{4,11,1}$
5->12	$M_{5,12,1}$
5->13	$M_{5,13,1}$
...	...

Fig. 7: Implementation of the LR-PON protection mechanism, showing the communication between nodes and Network Management System

is the direction away from the failure). In Fig. 7, the node experiencing a failure (node 0), sends a message to the NMS, indicating OLTs affected and failure type. From this information the NMS calculates the amount of load that needs to be protected and shared by each branch of the network (shown with different shades of grey in the figure, where the arrows indicate the direction the load is passed). The values in the load sharing tables indicate the amount of load that each node should pass on to their neighbours, and are populated considering the worst-case scenario of total node failure. For smaller failures, the value to offload is the minimum between the values in the tables and the remaining load to be shared on a given branch.

IV. Coverage optimization for a real geography

We have complemented our work with a case study of LR-PON deployment for a real geography, using data provided by the major Irish operator. The aim is to cover part or all local exchanges with a LR-PON deployment that provides dual-homing protection. The ILP formulation we employ to describe and solve the problem considers 20 MC nodes (although 18 is the minimum number of nodes required to achieve full and protected dual coverage of the country, we found that adding 2 nodes further reduces the overall protection capacity required). We consider different levels of coverage, expressed in terms of percentage of users covered, and there is no constraint in the maximum capacity of a MC node. The distance of the feeder fibre is calculated between the position of a candidate MC node and that of a local exchange, which becomes the location of the first-stage split. We allow an additional 6 km length for the span between the first splitter and the user. Although most "last-mile" links are within 2-3 km, we have opted for a more conservative choice (6 km is indeed the limit of commercial ADSL offers). However, while at 6km distance achievable ADSL bandwidth are exceptionally low (i.e., 640 Kbps downstream), the LR-PON provisioned bandwidth is distance independent. We consider two deployment strategies. The first minimises the overall fibre distance while the second minimises the protection capacity needed.

A. *Distance minimisation*

For the distance-based deployment strategy the objective is to place a number of MC nodes using a scheme that minimises the sum of the distances between the local exchanges and their corresponding primary and secondary MC nodes. This is considered a valid strategy for LR-PON because the long distance feeder fibre deployment is a significant contribution to the total cost of the PON installation.

Constants:
- E: set of exchange sites whose locations are fixed
- d: matrix where $d(i, j)$ is the Euclidean distance between the positions of local exchange sites i and j

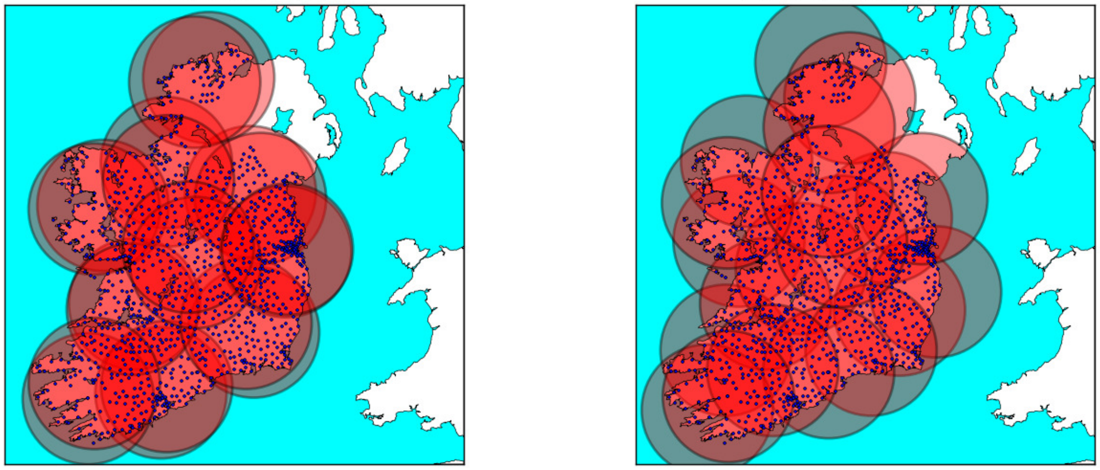
Variables:
- $M(j)$: position of a MC node j; if $M(j) = r$ then node j is located at the position of local exchange site r
- P_i: primary MC node of a local exchange site i
- S_i: secondary (i.e., backup) MC node of a local exchange site i

Constraints:
- $P_i \neq S_i$: the primary and secondary MC nodes of an exchange site i are different
- $(P_i = j) \implies \forall r((r \neq j) \Rightarrow d(i, M(j)) \leq d(i, M(r)))$: if j is a primary node of $i \in E$ then there does not exist any other node r such that the distance between the positions of i and r is less than the distance between the positions of i and j
- $(S_i = j) \implies \forall r((r \neq j \wedge r \neq P_i) \Rightarrow d(i, M(j)) \leq d(i, M(r)))$: if j is a secondary node of $i \in E$ then there does not exist any other node r such that r is not the primary node of i and the distance between the positions of i and r is less than the distance between the positions of i and j

Objective:
- minimise $\sum_{i \in E}(d(i, M(P_i)) + d(i, M(S_i)))$, i.e. the sum of the distances between local exchanges and their corresponding MC nodes.

B. *Protection capacity minimisation*

The objective of the second deployment strategy for placing MC nodes is to minimise the protection load needed in the network following the load-spreading mechanism previously described, subject to the constraint that each exchange site is



(a) Optimization based on distance minimisation

(b) Optimization based on protection-load minimisation

Fig. 8: Optimized deployment of LR-PON infrastructure in Ireland, providing dual-parented coverage for 100% of customers

connected to its two nearest MC nodes. The constants, variables and constraints of this model are basically the union of those of the models presented for capacity minimisation through load sharing (section III-C) and distance minimisation (section IV-A), with two exceptions. The constants Q_i and U_{ij} of the former model are now integer variables. The initial load of a MC node i is $Q_i = \sum_{P_e=i} l_e$, where l_e is the load (expressed in terms of number of users) of the exchange site e. This is basically the total number of customers that are connected to MC node i via their respective exchange sites. The upper bound on the load that can be transferred from a node i to another node j is equal to the sum of the loads of all exchange sites whose primary node is i and secondary node is j: $U_{ij} = \sum_{P_e=i \wedge S_e=j} l_e$.

Objective. The objective is to minimise the total amount of IP over-provisioning capacity required over all MC nodes for protection, i.e., $min. \sum_{i\in\mathcal{V}} M_i - Q_i$. It is also desirable to minimize the number of customers that are affected. Therefore, we use $\sum_{i\in\mathcal{V}} \alpha \times (M_i - Q_i) + \sum_{\forall i,j,k\in\mathcal{V}} T_{ijk}$ as the objective, where α is any constant that is greater than $\sum_{\forall i,j,k\in V} T_{ijk}$.

C. Approach

The problem of finding optimal node placement by minimising overall fibre distance either by minimising overall fibre distance or by minimising overall protection load required is NP-complete. The problem of finding optimal node placement by minimising overall fibre distance was formulated as a mixed integer programme and solved using CPLEX. The problem of finding optimal node placement by minimising overall protection load was decomposed into two phases. In the first phase we find a feasible placement of MC nodes using a mixed integer programing solver then use a constraint-based local search to improve the quality of the placement by reducing the overall protection required when the number of hops is restricted to 1. The process is repeated until the search terminates or the time spent reaches a given threshold. We avoid finding the same solution by adding cuts to the MIP solver and randomization to the local search. During the second phase we find a load transfer strategy that minimises the overall protection load when the number of hops is greater than 1.

D. Technical comparison

Figure 8 shows the LR-PON coverage results of our optimisation strategies. The small dots represent the positions of the local exchanges (i.e., where the first-stage splitters are located), which are connected, through dual homing, to one MC node for primary service and to a second MC node for protection. Hence the overlap between coverage areas of different MC nodes. We can easily see how the minimum distance strategy (Fig.8a) tends to provide primary and protection coverage by overlapping two almost concentric areas. Therefore its ability to share load among multiple network nodes is small. This can be likened to the situation in Fig. 2, with the addition that each node is duplicated. The minimum protection-load strategy instead (fig.8b) tends to separate nodes further apart, which, by creating multiple overlapped areas, increases the load sharing ability. In addition since primary and secondary nodes are further apart, the latter solution provides much better resilience against geographical disasters. The figure we have shown refers to a situation where 100% of users are covered by the LR-PON service.

Figure 9 is similar to Fig. 5 (which was obtained through simulated network scenarios) and shows how the percentage of IP protection load (calculated with respect to the total primary load) varies when the number of hops varies between 1 (load only spread to direct neighbours) and 8 (load spread among all the nodes in the network). Results are reported for different values of coverage, where, for example, a 90% coverage value indicates that we have selected the top largest local exchanges that cover 90% of the total number of customers. The customer distribution over the local exchanges is heavy-tailed, as reducing the coverage from 100% to 90% of customers corresponds to a 50% reduction in the number of local exchanges considered. When we consider coverage scenarios below 100%, the MC node selection process is not re-optimised. Rather the node location remains the same as in the 100% coverage case. This reflects a situation where an operator selects the locations for the MC nodes upfront, optimising for the 100% coverage scenario, and such locations remain unchanged throughout the deployment phase. The results we show for the 80% and 90% coverage cases quantify the sub-optimality during the initial phases of the deployment where the country is not fully covered by the LR-PON deployment.

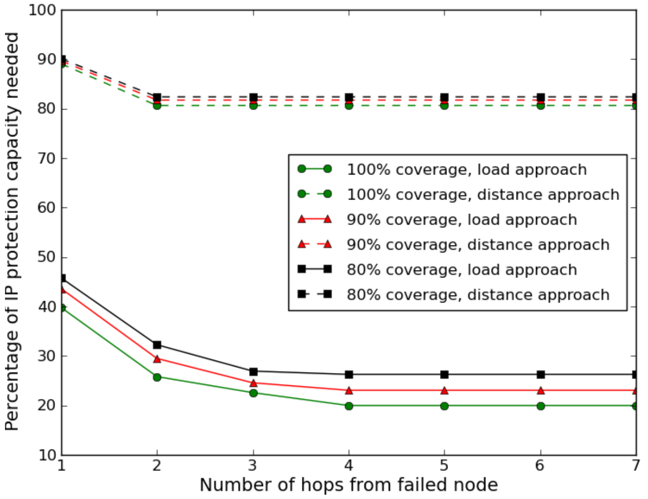


Fig. 9: Percentage of IP over-provisioning for protection capacity, in relation to the primary IP load, for a realistic deployment, for different coverage values

The main insight we gain from our results is that the minimum-load case shows much lower requirements for over-provisioning protection capacity with respect to distance minimisation. In the first case overprovision capacity is reduced by 80% compared to a 1+1 overprovisioning scenario, while in the second the reduction is much less noticeable (about 20%). As we observed in Fig. 8b, this is due to the larger distance between MC nodes that enables overlapping among a larger number of nodes, thus allowing protection traffic resulting from the failure of a MC node to be more easily offloaded and shared among the other MC nodes. The advantage of our proposed solution comes from the fact that we are considering as worst case the failure of any individual MC node, while we have ignored multiple simultaneous failures. Since the mechanism we propose offers an overall protection capacity that is much less than the overall primary capacity (i.e., about 80% less), multiple simultaneous failure will not be fully protected for. Although in principle a 1+1 protection scenario could offer full redundant capacity for the entire network, realistically, the type of disaster that could cause simultaneous failure of multiple metro-core nodes would probably also affect any secondary node, making any protection mechanism ineffective. We remind that due to the long optical reach any individual MC node covers an area of about 16,000km^2. Indeed, as previously mentioned, since our load-sharing mechanism places primary and secondary node further apart from each other, it guarantees a higher level of resiliency against geographical disaster (e.g., compared to scenarios were the protection nodes are co-located with the primary nodes or placed following a distance minimization strategy).

The second observation we make is that these results are comparable to those in Fig. 5 for a 20-node network obtained with a equal-node distribution (for lower number of hops) and to those obtained with a uniform traffic distribution (for higher number of hops). Even if the population distribution for Ireland is skewed, as over 25% of the population is located in the capital city (reaching almost 40% for the greater Dublin area), the optimisation process positions the nodes so that the number of users per MC node is relatively uniform. This is achieved by positioning a larger number of nodes around highly populated ares, as we can see in Fig. 8b around the Dublin area.

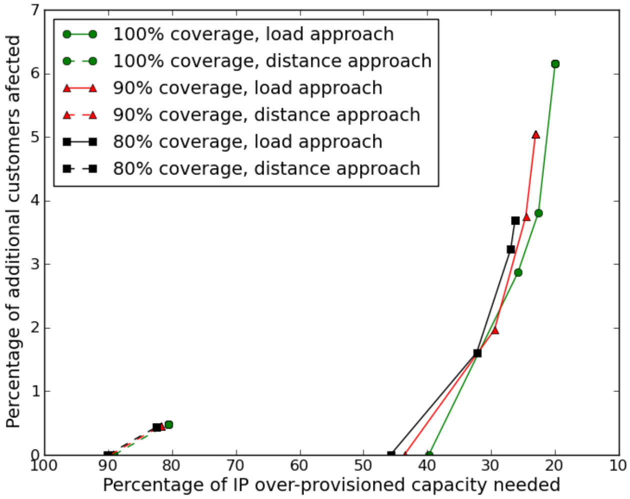


Fig. 10: Additional customers affected by a total node failure calculated for a realistic deployment, with 80, 90 and 100% coverage scenarios

Figure 10 shows the additional customers affected by a failure (values are averaged over all possible failures), because of the protection sharing operations. If full country coverage is assumed, the average number of additional customers affected by the process is just over 6%, while protection capacity is reduced by almost 80% compared to 1+1 protection. If the load is only shared within the first two hops from the failed node, the percentage of additional customers affected becomes less than 3%, while the capacity reduction is still about 75%. With respect to the distance-based approach, considering the 100% coverage case, we can see that the load-base approach can reduce overprovisioning by 52%, the percentage of customers affected being equal (i.e., considering a 0.4% value).

The practical relevance of the results shown in Fig. 10 strictly depends on the protection switching time. The dual-homing protection mechanism we have described requires switching customers between OLTs and an update of the IP routing tables. As already discussed in section III-D, it is not clear whether OLT protection can be achieved quickly enough (e.g., in the 50 ms range) to be unnoticeable to the users. If the switching mechanism requires longer then the transitory interruption that the load-sharing mechanism might produce could be tolerated only if it affects a small percentage of users and the cost benefits are sufficient to justify the impact on the customers. The values we have obtained between 3% and 6% for a realistic deployment scenario suggest the proposed approach is practical.

E. Economic comparison

The previous section showed how the load-based optimisation method can reduce the amount (thus the associated costs) of IP capacity over-provisioning for protection purposes. However such advantage comes at a cost, because load-based optimisation increases the total amount of fibre deployed, compared to the distance-based optimisation method. We have further examined such a trade-off by carrying out a detailed cost analysis. Our cost model is based on a modeling tool developed by one of the authors while working in BT. It considers the total LR-PON cost, including fibre deployment and transmission equipment. We have accounted for transmission equipment able to compensate for impairments arising from both the 100 km reach and the high splitting loss of a 512-way split. Both primary and secondary MC nodes are selected such that any local exchange they serve is within the optical reach of the system. The final cost is obtained by adding to the LR-PON cost, the cost incurred for both the primary (i.e., working) IP capacity and the additional IP capacity for protecting the nodes. The value of IP capacity needed on the network was obtained by multiplying the number of customers of all local exchanges covered by each MC node, by different average sustained bandwidth values, varying from 100Kbps (a typical average in today's networks) to 20 Mbps (the average sustained bandwidth of a single wavelength 10G LR-PON shared among 500 customers). We have also considered an average value of inter-node traffic of 50% (i.e, half of the traffic remains within any given metro/core node, while the other half crosses the node's boundaries). We do not provide cost comparison with architectures other than LR-PON, as this has been addressed in [8].

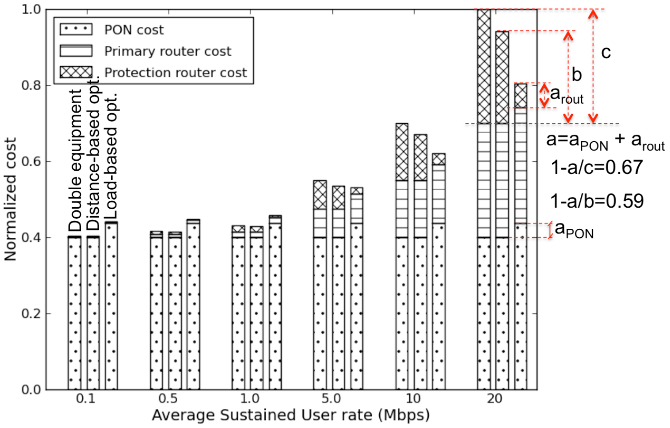


Fig. 11: Cost breakdown between LR-PON access network and IP protection capacity, for minimum distance and minimum load strategies, for a 100% coverage scenario

Figure 11 shows the normalized total cost per user of LR-PON deployment against the average sustained user bandwidth. The cost is also broken down in PON access costs (deployment and equipment), cost for the working (unprotected) IP routing and cost for IP protection. The three different columns for each bandwidth value represent (respectively from left to right), the scenario based on doubling protection equipment (where metro/core nodes are selected based on minimum distance optimization), the load sharing scenario based on distance minimisation, and the load sharing scenario based on load minimisation. From the figure we can see that for lower data rates the fibre deployment cost totally dominates over any other cost. The strategy based on distance minimisation seems thus more cost-effective. However for data rates above 2-3 Mbps, IP protection costs are not negligible and the load minimisation strategy yields better results.

We believe the results we have presented emphasize the advantage of combining the load-sharing algorithm we have designed with the deployment strategy based on the minimisation of protection IP load. The cost studies we presented show that our deployment strategy can reduce the overall network costs by about 20% compared to 1+1 protection. In Fig. 11 we also isolate the protection-related costs for the three scenarios: for the 1+1 (the c value) and distance-based (the b value) scenarios, the protection cost considered is only due to the increase in IP routers capacity (we remind the reader that we focus on this cost as it appears to be largely dominant over other costs). For the load-based scenario (the a value), in order to make a fair comparison, we consider the IP protection cost and the additional PON cost due to the fact that load-minimisation yields longer fibre distance (thus larger cost) compared to the other scenarios. The results show that for the 20Mbps case the load-sharing approach can save 59% of protection-related costs compared to distance minimisation and 67% compared to 1+1 protection. The 10Mbps case shows values, respectively, of 43% and 54%.

Although cost savings are not evident unless we consider average access rates above 2-3 Mbps, average user bandwidths will easily exceed such value over the lifetime of a fibre access network. For example 10 Mbps average busy period bandwidth can be expected over the next decade [8]. The current copper access network has been in service for well over half a century and we can assume a similar life-time for fibre-based access networks. From a technical point of view, average rates higher than 20 Mbps can easily be achieved by adding more wavelengths to the existing LR-PON infrastructure, a solution known as hybrid WDM-TDM PON upgrade. Although we haven't examined costs for multi-wavelength LR-PON, since the deployment cost for additional wavelengths is extremely small compared to the initial PON deployment, we can infer that as additional wavelengths (and therefore increasing traffic) are introduced into the PON network, the cost saving in IP protection equipment allowed by our load-sharing approach will increase well above the values we have presented for the single wavelength scenario.

V. CONCLUSIONS

In this work we have shown that when considering a Long-Reach Passive Optical Network deployment strategy, significant cost savings can be achieved by optimising the network design and layout such that protection capacity is minimised rather than simple distance minimisation. Since LR-PON also replaces the current back-haul network, protection must in fact be take into account. We have first proposed a mechanism that reduces the IP protection capacity needed at each node, by sharing the protection load resulting from a failed node over the entire network (or part of it). We have then shown that a metro-core nodes deployment strategy based on minimisation of IP protection capacity yields sensibly reduced costs. One of the main outcomes of our work is that we show that fibre access deployment strategies need to be well thought out in advance of their implementation and must consider network protection at the outset.

Acknowledgment

This work is supported by Science Foundation Ireland Grant No. 10/CE/I1853. We would like to thank Eircom for providing information about their internal network structure.

References

[1] Cisco Systems Inc, *Cisco Visual Networking Index: Forecast and Methodology, 2009-2014*

[2] D. B. Payne, *World bandwidth growth over the next decade is it viable?*, CIP Technologies white paper, 2008.

[3] A. M. Hill, R. Wyatt, J. F. Massicott; K. Blyth, D. S. Forrester, R. A. Lobbett, P. J. Smith and D. B. Payne, *39.5 million-way WDM broadcast network employing two stages of erbium-doped fibre amplifiers*, IEEE electronic letters, (26) 22, 1882-1884, 1990.

[4] D. B. Payne and R. P. Davey, *The future of fibre access systems?*, BT Technology Journal, (20) 4, 104-114, 2002

[5] C. Bouchat, C. Martin, E. Ringoot, M. Tassent, I. Van de Voorde, B. Stubbe, P. Vaes, X. Z. Qiu and J. Vandewege, *Evaluation of SuperPON demonstrator*, in proceedings of IEEE LEOS, paper ThC 2.3, 2000

[6] P. D. Townsend, G. Talli, E. K. MacHale and C. Antony, *Long reach PONs*, in proceedings of IEICE COIN, 2008.

[7] D. Nesset, D. B. Payne, R. P. Davey and T. Gilfedder, *Demonstration of Enhanced Reach and Split of a GPON System Using Semiconductor Optical Amplifiers*, in proceedings of IEEE ECOC, 1-2, 2006.

[8] D. B. Payne, *FTTP deployment options and economic challenges*, in proceedings of IEEE ECOC, paper 1.6.1, 2009

[9] H. Song, K. Byoung-Whi and B. Mukherjee, *Long-reach optical access networks: A survey of research challenges, demonstrations, and bandwidth assignment mechanisms*, IEEE Communications Surveys & Tutorials, 12(1):112-123, 2010

[10] K. I. Suzuki, Y. Fukada, D. Nesset and R. Davey, *Amplified gigabit PON systems*, Journal of Optical Networking, 6(5):422-433, 2007

[11] M. O. Van Deventer, J. D. Angelopoulos, H. Binsma, A. J. Boot, P. Crahay, E. Jaunart, P. J. M. Peters, A. J. Phillips, X. Z. Qiu, J. M. Senior, M. Valvo, J. Vandewege, P. J. Vetter and I. Van de Voorde, *Architecture for 100 km 2048 split bidirectional SuperPONs from ACTS-PLANET* in proceedings of SPIE, 2919, 245-251, 1996.

[12] R. P. Davey, P. Healey, I. Hope, P. Watkinson, D. B. Payne, O. Marmur, J. Ruhmann and Y. Zuiderveld, *DWDM Reach Extension of a GPON to 135 km*, in proceedings of IEEE/OSA OFC, 2005.

[13] T. Nakanishi, K I. Suzuki, Y. Fukada, N. Yoshimoto, M. Nakamura, K. Kato, K. Nishimura, Y. Ohtomo and M. Tsubokawa, *High sensitivity APD burst-mode receiver for 10Gbit/s TDM-PON system*, IEICE Electronics Express, 4(10):588-592, 2007

[14] G. Talli, C. W. Chow, P. Townsend, R. P. Davey, T. De Ridder, X. Z. Qiu, P. Ossieur, H. G. Krimmel, D. Smith, I. Lealman, A. Poustie, S. Randel and H. Rohde, *Integrated Metro and Access Network: PIEMAN*, in proceedings of European Conference on Networks and Optical Communications, 2007

[15] H. Song, A. Banerjee, K. Byoung-Whi and B. Mukherjee, *Multi-thread polling: a dynamic bandwidth distribution scheme in long-reach PON*, IEEE JSAC, 27(2):134-142, 2009

[16] M. Ruffini, D. B. Payne and L. Doyle, *Protection strategies for long-reach PON*, in proceedings of ECOC 10, paper Tu.5.B.2

[17] ITU-T, *Gigabit-capable passive optical networks (GPON): General characteristics*, Recommendation G.984.1, 2008

[18] A. J. Phillips, J. M. Senior, R, Mercinelli, M. Valvo, P. J. Vetter, C. M Martin, M. O. Van Deventer, P. Vaes and X. Z. Qiu, *Redundancy strategies for a high splitting optically amplified passive optical network*, Journal of lightwave technology, 19(2):137-149, 2001.

[19] B. W. Kim, *Introduction to WDM-PON and WE-PON*, Working document, ETRI, 2007.

[20] J. A. Lazaro, J. Prat, P. Chanclou, G. M. Tosi Beleffi, A. Teixeira, I. Tomkos, R. Soila and V. Koratzinos, *Scalable Extended Reach PON*, in proceedings of IEEE/OSA OFC, paper OThL2, 2008.

[21] D. K. Hunter, Z. Lu and T. H. Gilfedder, *Protection of long-reach PON traffic through router database synchronization*. Journal of Optical Networking 6(5):535-549, 2007

[22] P. Sebos, J. Yates, G. Li, D. Wang, A. Greenberg, M. Lazer, C. Kalmanek and D. Rubenstein, *Ultra-fast IP link and interface provisioning with applications to IP restoration*, in Proceedings of the 2007 IFIP international conference on Network and parallel computing

[23] M. de Berg, O. Cheong, M. van Kreveld and M. Overmars, *Computational Geometry: Algorithms and Applications*, edited by Springer-Verlag, 2000.

[24] http://www-01.ibm.com/software/integration/optimization/cplex-optimizer/

[25] D. Mehta, B. O'Sullivan, L. Quesada, M. Ruffini, D. Payne and L. Doyle, *Designing Resilient Long-Reach Passive Optical Networks*, in proceedings of conference on Innovative Applications of Artificial Intelligence, 2011.

[26] J. Kang, M. Wilkinson, K. Smith and D. Nesset, *Restoration of Ethernet Services over a Dual-Homed GPON System*, in proceedings of OSA OFC, paper NWD2, 2008.

Dr. Marco Ruffini is currently an assistant professor on optical network architectures at the department of computer science of the University of Dublin, Trinity College, where he obtained his PhD in 2007, pioneering the concept of Optical IP Switching. He is part of the CTVR telecommunication research centre and his research interests include low-based optical switching, experimental optical testbeds, long-reach PON, cross-layer and cognitive optical networks, and techno economic studies of next-generation transparent architectures. He worked on wireless inter-vehicle communications at Philips Research Laboratories in Aachen (2003-2005). He holds a degree in electronic engineering from Universita' Politecnica delle Marche in Italy (2002). He has authored over 25 international journals and conference publications and 8 patents.

Dr. Deepak Mehta received his PhD in computer science from University College Cork in 2009 for his work on generic arc consistency algorithms in constraint programming. His PhD work was supported by Boole Center for Research in Informatics. He has been working as a research scientist in Cork Constraint Computation Center since March 2007. He worked on the project on personalization of context-aware telecommunication services for three years. This project was funded by IRCSET-Embark Initiative and British Telecom. From March 2010 he has been working on network optimisation problems, which are undertaken in Centre for telecommunications Value-Chain Research (CTVR).

Professor Barry O'Sullivan holds the Chair in Constraint Programming at University College Cork. He is Director of the Cork Constraint Computation Centre in the Computer Science Department at UCC, SFI Principal Investigator, President of the Association for Constraint Programming, Chairman of the Artificial Intelligence Association of Ireland, Coordinator of the EuropeanResearch Consortium for Informatics and Mathematics Working Group on Constraints, and Executive Council member of the Analytics Society of Ireland.

Dr. Luis Quesada received his PhD in computer science from Université Catholique de Louvain in 2006 for his work on solving constrained graph problems using global constraints based on the notion of dominators. Since January 2007, he works as a research scientist at the Cork Constraint Computation Centre, a world-leading research centre dedicated to large-scale complex optimisation. During his first three years at 4C, he worked on the personalization of context-aware telecommunication services. Since January 2010, he works on the solutions of combinatorial optimization problems that arise from the configuration of telecommunication networks in the CTVR project. During his PhD studies he was one the research assistants of MISURE, a project with the European aerospace industry whose goal was to develop a system capable of automatically managing the mission of an uninhabited air vehicle. Dr Quesada has been invited lecturer at Pontificia Universidad Javeriana (Colombia) and teaching assistant at both Université Catholique de Louvain (Belgium) and at the University of Melbourne (Australia).

Professor Linda Doyle is a member of faculty in the School of Engineering, Trinity College, University of Dublin Ireland. She is currently the Director of CTVR, the Telecommunications Research Centre. CTVR is a national research centre that is headquartered in Trinity College and based in five other universities in Ireland. CTVR carries out industry-informed research in the area of elecommunications and focuses both on wireless and optical communication systems. Prof. Doyle is responsible for the direction of the CTVR as well as running a large research group that is part of the centre. Her research group focuses on cognitive radio, reconfigurable networks, spectrum management and telecommunications and digital art.

Professor David B. Payne joined CTVR in Trinity College Dublin in February 2010. Before this he was a principal consultant to BT group on optical networks where he was responsible for strategic guidance and direction on optical network architectures to BT Group CTO and BT Openreach strategy. In the past number of years he has been the Senor Industrial Advisor at the Institute of Advanced Telecommunications at Swansea University where he provided network architecture expertise in order to establish collaborative links with BT Research. He has over 20 patents (several now lapsed) and over 60 publications (journal articles, electronics let-ters, optics letters, conference colloquium publications, 25 invited papers, contributions to 7 books, two in progress).