Protection strategies for Next Generation Passive Optical Networks -2

Abhishek Dixit, Mozhgan Mahloo, Bart Lannoo, Jiajia Chen, Lena Wosinska, Didier Colle, Mario Pickavet

Abstract— **Next Generation Passive Optical Networks-2 (NG-PON2) are being considered to upgrade the current PON technology to meet the ever increasing bandwidth requirements of the end users while optimizing the network operators' investment. Reliability performance of NG-PON2 is very important due to the extended reach and, consequently, large number of served customers per PON segment. On the other hand, the use of more complex and hence more failure prone components than in the current PON systems may degrade reliability performance of the network. Thus designing reliable NG-PON2 architectures is of a paramount importance. Moreover, for appropriately evaluating network reliability performance, new models are required. For example, the commonly used reliability parameter, i.e., connection availability, defined as the percentage of time for which a connection remains operable, doesn't reflect the network wide reliability performance. The network operators are often more concerned about a single failure affecting a large number of customers than many uncorrelated failures disconnecting fewer customers while leading to the same average failure time. With this view, we introduce a new parameter for reliability performance evaluation, referred to as the failure impact. In this paper, we propose several reliable architectures for two important NG-PON2 candidates: wavelength division multiplexed (WDM) PON and time and wavelength division multiplexed (TWDM) PON. Furthermore, we evaluate protection coverage, availability, failure impact and cost of the proposed schemes in order to identify the most efficient protection architecture.**

Index Terms— **Resilience; Availability; WDM-PON; TWDM-PON**

I. Introduction

THE bandwidth requirements of the end users are on increase, which brings the need for next generation passive optical networks 2 (NG-PON2). The PON technology uses an optical line terminal (OLT) at the central office (CO) and an optical network unit (ONU) at the user's premises, connected through an optical distribution network (ODN) in a tree topology. The two important candidates of NG-PON2 are wavelength division multiplexed PON [1] (WDM-PON) and time and wavelength division multiplexed PON (TWDM-PON) [2], [3]. These two flavors are chosen by the full service access network (FSAN) group [3]: TWDM-PON as the primary candidate of NG-PON2, and WDM-PON as the secondary candidate of NG-PON2 for the scenario where a high quality of service (QoS) is required.

WDM-PON increases the capacity of the current PON solutions (mainly time division multiplexed (TDM), e.g., EPON, GPON, XGPON) by using a wavelength layer in conjunction with a passive ODN. Out of many flavors of WDM-PON, we assume wavelength routed WDM-PON, using an arrayed waveguide grating (AWG) in the remote node (RN) to multiplex/demultiplex wavelengths and route a wavelength pair (up- and downstream) to each ONU. WDM-PON gives a dedicated wavelength to a user, alleviating complexity of TDM and assuring a high QoS. However, the users may not permanently need this high dedicated bandwidth and thus, it could be better shared among users. TWDM-PON accomplishes that by sharing the capacity of a WDM-PON in time domain (i.e., using TDM). TWDM-PON utilizes a power splitter (PS) at the RN, which broadcasts wavelengths to all ONUs. Since multiple wavelengths are available at ONUs, tunable receivers are required.

NG-PON2 faces more challenges in achieving a high reliability performance than the conventional PON as it has longer fiber lengths with a higher fiber cut probability, there are more customers on a single PON segment, and it includes components with a higher complexity (tunability etc) and thus with a poorer reliability performance. Moreover, the level of protection required depends upon the user's profile. Businesses are run over fully protected networks and business users like to have full protection coverage [4]. Generally, there is a service level agreement (SLA) between business users and network providers by which the latter have to pay a penalty for service interruption. Thus, network providers like to minimize this penalty as much as possible by increasing protection for business users. Protection involves duplicating facilities like optical fiber paths, OLT cards, IP capacity and others. If all facilities are duplicated, the cost per user increases significantly. This large incremental cost hurts the interest of residential users who prefer low cost of service. Thus, while

The research leading to these results has received funding from the European Community's Seventh Framework Program (FP7/2007-2013) under grant agreement n° 249025 (ICT-OASE) and n° 318137 (ICT-DISCUS).

Abhishek Dixit, Bart Lannoo, Didier Colle, and Mario Pickavet are with the Department of Information Technology, Ghent University-iMinds, Ghent, Belgium (email: abhishek.dixit@intec.ugent.be).

Mozhgan Mahloo, Jiajia Chen, and Lena Wosinska are with KTH Royal Institute of Technology, Kista, Sweden (email: mahloo@kth.se).

providing high protection coverage to business users, the residential users must be shielded from a high cost increase.

Our previous works in [5] and [6] focus on the efficient protection schemes for TWDM-PONs. In this paper, we propose reliable architectures (section III) for both WDM- and TWDM-PON and evaluate (section IV) reliability performance and cost of the proposed architectures. Also, we propose a new metric for reliability performance evaluation, referred to as failure impact (FI) (section II).

II. Parameters For Reliability Performance Evaluation

In this section, we discuss the four parameters considered for the reliability performance measurement: protection coverage, availability, FI and cost.

A. *Protection Coverage*

Protection coverage measures the percentage of duplicated architectural elements (i.e. components and fibers). If all elements are doubled, the network has a protection coverage of 100%. As some elements will only be duplicated for business users, the protection coverage will be different for business and residential users.

B. *Component and Connection Availability*

Asymptotic availability is defined as the probability that a component is operable at an arbitrary point of time and can be expressed as:

$$A = 1 - \frac{\mathrm{MTTR}}{\mathrm{MTBF}} \tag{1}$$

with: MTTR = mean time to repair,
MTBF = mean time between failures.

Connection availability means the probability that a logical connection (e.g. between the OLT and ONU) is operable. The desired value of the availability depends on the network operator and the customers in operation. However, as the aggregation networks are built with an availability of 'four nines' [7], we feel that a similar availability is sufficient for NG-PON2 networks.

C. *Failure Impact (FI)*

Besides availability, we consider another resilience parameter, namely the failure impact (FI), which is an improvement over the figure of merit (FOM) introduced in [8] and the failure impact robustness (FIR) introduced in [6]. The parameter provides a weight to the number of failures in the network, thus modeling the impact of a failure in an irrational environment, where a network operator is worried more about a big failure disconnecting all clients for 1 hour at the same time (negative release on press, newspapers, TV leading to bad publicity) than for multiple small failures throughout the year disconnecting every client for 1 hour on average.

Impact of a failure in a rational environment [9] is proportional to the number of customers disconnected by the failure, N, and the unavailability of the component, U. This leads to the definition:

$$\mathrm{FI} = N \times U \tag{2}$$

E.g., Case 1: N =1000 customers, $U = 10^{-5}$; Case 2: N =100, $U = 10^{-4}$ have the same rational impact.

To model the impact of failures in an irrational environment, we assume that all failures are statistically independent and all failures have a binary consequence: connection is fully disconnected (0) or not (1), no intermediate situations are considered. The FI in an irrational environment is given by:

$$\mathrm{FI} = N^{\alpha} \times U \tag{3}$$

where $\alpha > 1$ (growing α leads to more and more irrationality) and $\alpha = 1$ is the rational situation. The parameter α denotes "irrationality" in the behavior of network operators and cannot be determined by analytical interpretations. Models studying the psychological attributes of human behavior can be used to indicate the value of α. E.g., Case 1: N =1000 customers, $U = 10^{-5}$; Case 2: N =100, $U = 10^{-3}$ have the same irrational impact (if α =2). In case of different non-simultaneous events, the impact of these events can be summed, leading to additivity. Note that we also could define the FI as: $\mathrm{FI} = N \times U^{1/\alpha}$, but then we would lose the additivity characteristic.

The generalized function for failure impact can be deduced as: $\mathrm{FI} = \mathrm{f}(N) \times U$, with $\mathrm{f}(N)/N$ monotically growing in N, and when α (factor of irrationality) =1, $\mathrm{f}(N) = N$.

Impact of combination of errors:

To investigate the effect of a combination of errors, let us assume that there are two events f_1 and f_2, with unavailability U_1 and U_2, and the number of customers being affected as N_{1s} and N_{2s} respectively when the events occur separately and the number of customers being affected as N_p when the two events occur simultaneously.

The impacts of errors when they occur separately are FI_1 and FI_2 respectively and can be given as:

$$\mathrm{FI}_1 = N_{1s}^{\alpha} \times U_1 \times (1 - U_2) \tag{4}$$

$$\mathrm{FI}_2 = N_{2s}^{\alpha} \times U_2 \times (1 - U_1) \tag{5}$$

If they occur simultaneously, the FI is:

$$\mathrm{FI}_3 = N_{p}^{\alpha} \times U_1 \times U_2 \tag{6}$$

By combining Eq. (4), (5) and (6), the total FI is given as:

$$\mathrm{FI}_{Total} = N_{1s}^{\alpha} \times U_1 \times (1 - U_2) + N_{2s}^{\alpha} \times U_2 \times (1 - U_1) + N_{p}^{\alpha} \times U_1 \times U_2 \tag{7}$$

Assuming $U_1 \times U_2 \approx 0$, and $1 - U_i \approx 1$, the total FI is:

$$\mathrm{FI}_{Total} \approx N_{1s}^{\alpha} \times U_1 + N_{2s}^{\alpha} \times U_2 = \mathrm{FI}_1 + \mathrm{FI}_2 \tag{8}$$

We can apply this definition of the FI to more specific examples. Let us first consider two parallel links, with unavailability U_1 and U_2, protecting N customers. In case of parallel protection, since no customer gets affected by a single failure $N_{1s} = 0$, $N_{2s} = 0$, and $N_p = N$. Thus Eq. (7) could be expressed as:

$$\text{FI}_{Total} = N^{\alpha} \times U_1 \times U_2 \tag{9}$$

Let us now consider two serial links with unavailability U_1 and U_2 and the number of customers connected to each link as N_1 and N_2 respectively. For simplicity, let us again assume that $N_1 = N_2 = N$. In case of serial connection, $N_{1s} = N_{2s} = N_p = N$. Thus, Eq. (7) reduces to:

$$\text{FI}_{Total} = N^{\alpha} \times (U_1 + U_2 - U_1 \times U_2) \tag{10}$$

D. Cost

The primary incentive of protection for network operators is a huge cost that they otherwise have to pay, especially to business users, in the form of a penalty for a loss of service in an event of a failure. Resilient networks increase network availability and hence reduce this penalty which is a part of the operational expenditures of the network. However, protection also increases other components of costs, like cost due to duplicated network equipment, infrastructure and others. The optimal resilient scheme is the one that minimizes the total cost of ownership of the network.

There are primarily two components of costs: capital expenditures (CAPEX) and operational expenditures (OPEX). CAPEX involves cost in network equipment, equipment installation and network infrastructure.

- Network equipment: It is the cost due to passive or active equipment like an OLT, an ONU, an AWG and a PS.
- Equipment installation: It is the cost required in installing network equipment which depends upon the number of technicians, the time to install and the travelling time. Note that this cost will not differ for a protected or unprotected case, and thus is not considered.
- Network infrastructure cost: It is the cost in installing fiber, which accounts for costs due to trenching, cabling, splicing etc.

OPEX involves the cost related to the maintenance of the network and is strongly dependent on the operating horizon (T_s), i.e., the time span for which a network is operable. It includes costs due to failure reparation, power consumption, floor space, and penalty paid to business users during an event of a failure. Note that except for penalty costs, all the other costs could increase with protection.

- Failure reparation: The failure reparation cost (C_{FR}), which involves the cost required in changing the equipment (or repairing the fiber) and the technician cost, depends upon how often a failure happens ($T_s/MTBF$), the equipment/fiber cost C_E, mean time to repair (MTTR)[1] and the technicians' salary (S_T).

$$C_{FR} = \frac{T_s}{MTBF}(C_E + MTTR \times S_T) \tag{11}$$

- Power consumption: The cost of power consumption of a component is evaluated as the product of power consumption P_E of a component, the cost of using power C_P, and the time span.

$$C_{PC} = P_E \times C_p \times T_S \tag{12}$$

- Floor space: The OLT's equipment occupies a space in the CO for which a yearly rental has to be paid. To evaluate this cost, we have to find out the slot space that each component requires within an OLT rack. From the knowledge of the size occupied by the rack, we can calculate the total area per CO, which determines the yearly rental.
- Penalty: Cost penalty paid to a user depends upon the connection unavailability, operating horizon, and cost penalty paid to a user per hour to compensate service interruption ($\overline{P}$).

$$C_{Pl} = U \times T_s \times \overline{P} \tag{13}$$

III. Reliable Architectures

To understand the reliability performance in the context of NG-PON2 architectures, first, we present the results of the analysis of the unavailability of various components in Fig. 1. The feeder fiber (FF) has the lowest availability and thus the basic protection strategy is to protect the FF. After the FF, the OLT has the worst availability and it should be protected. Both OLT and FF affect all customers and should be primarily protected. On the other hand, other PON segments do not affect all customers, and thus should only be protected for business users. Based on this learning, we consider four protection schemes for WDM- and TWDM-PON.

A. Protection scheme A

In protection scheme A (Fig. 2 A), the FF is protected, which impacts both business and residential users. Additionally, for business users, its distribution fiber (DF) and the ONU transceiver are also protected; the ONU transceiver, being an active element, has a high unavailability.

This configuration requires an extra switch at the OLT, whose configuration differs for WDM- and TWDM-PON. For WDM-PON, the switching to a protected fiber (PF) is not that straightforward. When switching from one feeder fibre port of the 2:N AWG at the RN to the second (and given that these are adjacent ports of an M:N device), while keeping the OLT wavelengths the same, a wavelength shift by one channel occurs at all AWG fan-out ports in the downstream direction. By default, then, the downstream signals would be routed to the wrong ONUs. In the upstream direction, the second feeder fibre port would remain dark if the ONUs retained their original working wavelengths. The second feeder fibre can be lighted correctly and the downstream wavelength shift can be compensated by *re-tuning* both the OLT and the ONUs by one channel. The retuning of the wavelengths at the ONUs can be accomplished by using embedded communication channels (ECC). We propose the switch for WDM-PON (Fig. 2) consisting of two mechanical switches. The two input ports are needed to collect wavelengths from two different output ports

[1] MTTR only includes repair and travelling time of the technicians.

of the multiplexer (which is also an AWG) at the OLT.

For TWDM-PON, a possible configuration of the switch may use an EDFA with a mechanical fiber switch. Using a simple 3 dB splitter will corrupt the data on the FF and PF.

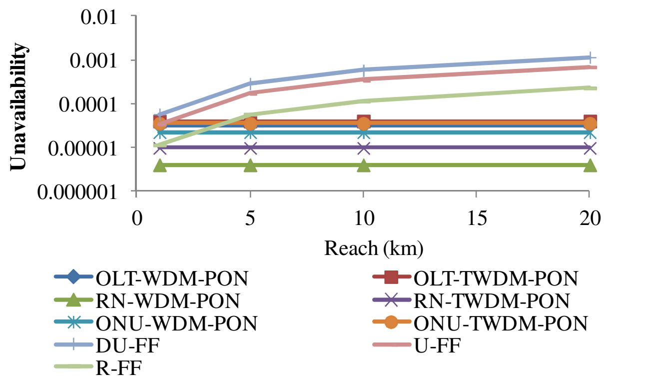


Fig. 1: Unavailability of various elements of WDM- and TWDM-PON. The unavailability numbers are from [10].

B. *Protection scheme B*

In protection scheme B (Fig. 2 B), both the OLT and the FF are protected for all users. As in scheme A, a business user has an additional protection of the DF and ONU transceivers. A backup OLT is used to protect *N* OLTs to save the protection cost. We assume a dual-parented (or dual-homed) approach to protect the OLT, in which the working and backup OLTs are geographically separated. This provides a higher level of reliability performance because it leads to independent power outage failures and increases the network reliability performance against local disasters. Moreover, the PF follows a disjoint geographical route to provide maximal protection against a cable cut, and thus, any cost savings because of the two OLTs at the same physical location (duplex approach) are minimal. Dual-parented scheme needs inter-OLT signaling to control the switching for protection. The OLTs are already interconnected through the aggregation network, which facilitates the inter- OLT signaling.

We assume full OLT duplication, including components such as switch, power supplies, and booster/preamplifier, because of the low availability of these active components. We also consider OLTs being directly connected to FFs. Note that they could always be connected through a 3dB splitter. However, the latter scheme needs an additional coupler, degrades the connection availability and FI, and requires extra fibers for a dual parented scenario.

C. *Protection scheme C*

Protection scheme C (Fig. 2 C) provides 100%[2] protection coverage for business users, by providing two duplicated parallel network segments. However, this approach is not beneficial for residential users as they have no protection. However as protection is only important for business users, this scheme is optimal to provide 100% protection coverage to business users and cheap access to residential users.

D. *Protection scheme D*

Protection scheme D (Fig. 2 D) provides 100% protection coverage to business users, and OLT and FF protection for residential users. The scheme uses two extra PSs before the remote node.

IV. ARCHITECTURAL EVALUATION

A. *Evaluation methodology*

The evaluation methodology involves calculating the availability, FI, and costs for the various technologies. The cost, MTBF, MTTR and power consumption values are taken from [10]. WDM- and TWDM-PON are assumed with a fan out of 32 and 512 respectively. The cost of penalty is assumed as 2 cost units (CU) per hour, where a CU denotes the cost of a GPON ONU. The parameter α is chosen as 2. The population of business users is assumed as 20%. For evaluating the infrastructure cost, a standard geometrical model like the Manhattan model is adopted and the design parameters are considered as in [11]. For modeling the floor space, we assumed a model presented in [11]. The availability and FI are calculated for three scenarios: dense urban (DU), urban (U), and rural (R). Besides, we also considered the performance for both business users (BUs) and residential users (RUs). The assumed lengths for the FF and PF and downtime are given in Table I.

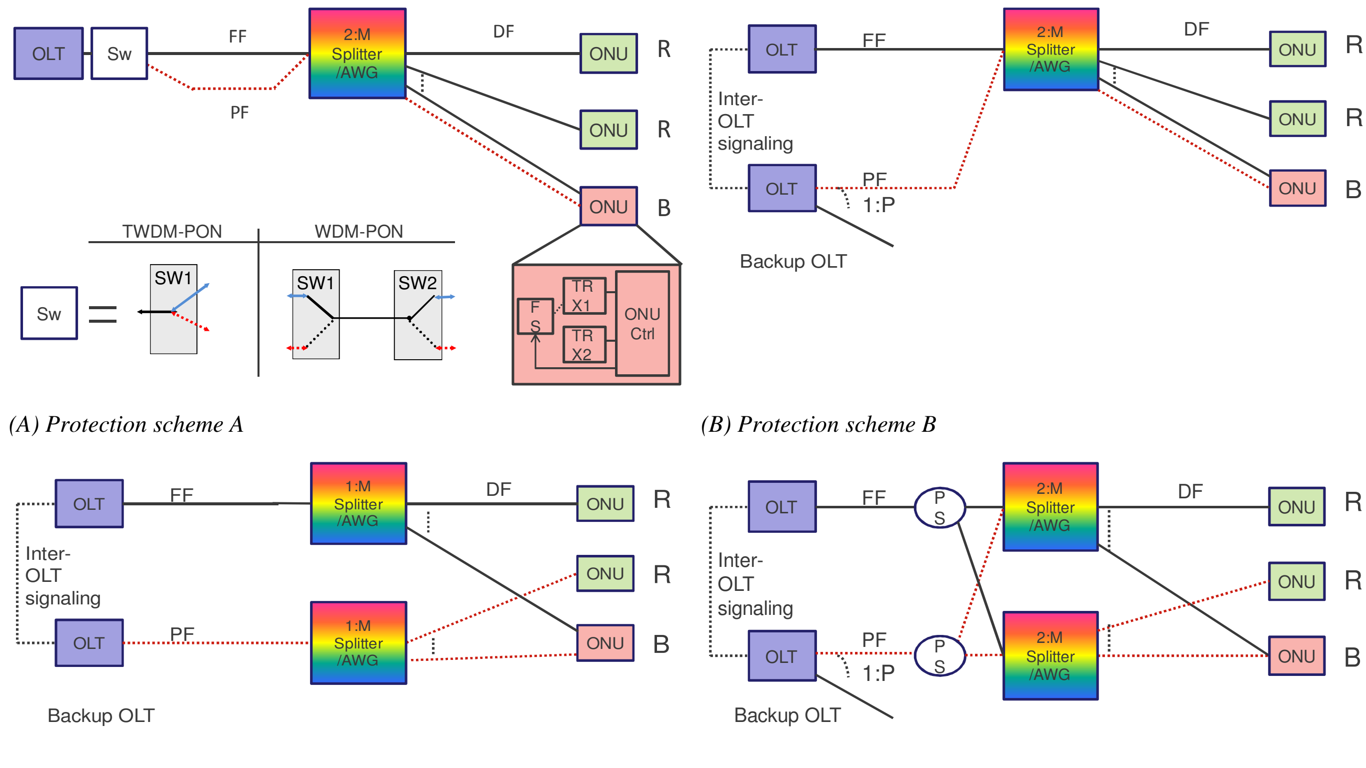
B. *Results*

First, we present the protection coverage of different schemes (Fig. 3). The protection schemes achieve the same protection coverage for WDM- and TWDM-PON. As the protection scheme moves from A to D, the protection coverage increases for business users, and the protection schemes C and D achieve 100% protection coverage. The protection scheme C, however, does not offer any protection to residential users.

The unavailability of various schemes in WDM- and TWDM-PON is shown in Fig. 4 for three population densities. The urban scenario has the lowest availability because of a combination of longer fiber lengths (compared to dense urban) and fiber downtime (compared to rural). There is no significant difference (limited to 3×10^{-5}) between the availability of WDM- and TWDM-PON; however, WDM-PON has a slight edge, which can be attributed to more complex tunable ONUs used in TWDM-PONs. The protection schemes from A to D decrease the unavailability for business users. The protection schemes achieve an availability of more than four nines for business users, with a best case availability of 0.99998.

The FI is shown in Fig. 5 for WDM-and TWDM-PON for three population densities. It is calculated for the total network and cannot be differentiated for residential or business users.

[2] It can also be argued that protection schemes C and D do not achieve 100% protection coverage as all components are not 100% duplicated, e.g., fiber switch in an ONU is not duplicated. However, the protection coverage provides a quick estimate of the network reliability performance and obviously does not respond to every minor intricacy.



(A) Protection scheme A

(B) Protection scheme B

(C) Protection scheme C

(D) Protection scheme D

Fig. 2: Protection schemes for WDM- and TWDM-PON. R = Residential users, B = Business users. Solid black line denotes FF and dashed red line denotes PF

The FI now clearly differentiates between WDM- and TWDM-PON. Even though WDM- and TWDM-PON have nearly the same availability, TWDM-PON has a FI about 200 times higher than WDM-PON. This is due to a high customer aggregation (512) in TWDM-PON, which makes it vulnerable to large impacts. An interesting observation about the FI and its relation to α (irrationality factor) can be seen in Fig. 6. Here we show the FI of various protection schemes relative to the unprotected scheme with varying α. Obviously all protection schemes decrease the FI, but the difference in the protection schemes generally broadens with more irrationality. Also, some protection schemes perform better with increased irrationality, e.g., scheme C has a lower FI than scheme B for a larger α. This can be attributed to a possible complete network black out in scheme B compared to scheme C where business customers are double protected.

The total cost per total number of users in the different protection schemes is evaluated in Fig. 7. How this cost is to be distributed among business and residential users will depend upon the business models. The analysis is done for the DU scenario. The choice of the scenarios does not significantly affect the relative results. We evaluated six components of the cost: penalty, floor space, power consumption, failure reparation, infrastructure, and equipment. The cost for penalty forms the significant portion of the total cost and decreases as protection coverage increases. For these results, the penalty paid to residential users is neglected. However, as the dependence of users on the Internet is growing, the network operators may be forced to pay a penalty to even residential users, incentivizing the network protection even more. All other components of costs increase as the level of protection increases from A to D, note the logarithmic scale of the y-axis. Emphatically, the total cost per user decreases with the increased level of protection, when operators pay a reasonable penalty of about 2 CU/hour to business users. Clearly, this proves that there is a major incentive for network providers to implement protection. Of course, if there is no associated penalty with a failure, no protection is required. The breakeven point is at a penalty of 0.06 CU/hour, which is fairly low and asserts the need of protection for the cost effective deployment of access networks.

V. Conclusions

We proposed four different protection schemes to improve reliability performance of two NG-PON2 candidate technologies: WDM- and TWDM-PON. The proposed schemes realize a protection level which varies from no protection to end-to-end protection for business users, and OLT and FF protection for residential users. We also proposed a new metric for reliability performance evaluation, namely failure impact. The proposed schemes are analyzed considering protection coverage, availability, failure impact and cost, in different populated scenarios. The analysis proves that unavailability, FI and the total cost of ownership is reduced significantly by the protection schemes. Of course, the cost is influenced by the penalty paid to business users for a loss of service, however, even for a meager cost penalty of ca. 0.06 CU/hour, the reliable architectures are mandated for a cost effective deployment. Although the unavailability of WDM- and TWDM-PON is nearly equal, we noticed a much higher failure impact for TWDM-PON because of its higher customer aggregation.

TABLE I. PARAMETERS OF FIBER LENGTHS IN DIFFERENT POPULATED SCENARIO: DENSE URBAN (DU), URBAN (U) AND RURAL (R)

Scenario	DU	U	R
Downtime (h)	0.5	0.3	0.1
WP	1	4	9.5
BP	3.5	12	28
DF	1.5	2.5	3.5

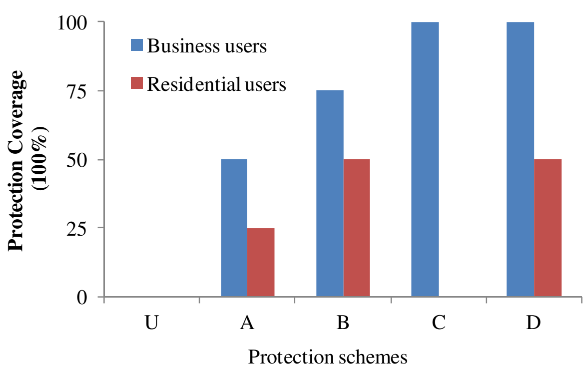


Fig. 3: Protection coverage of different schemes for WDM- and TWDM-PON

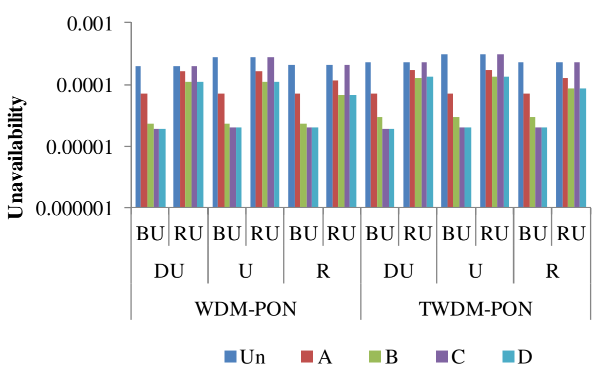


Fig. 4: Unavailability of different schemes for WDM- and TWDM-PON

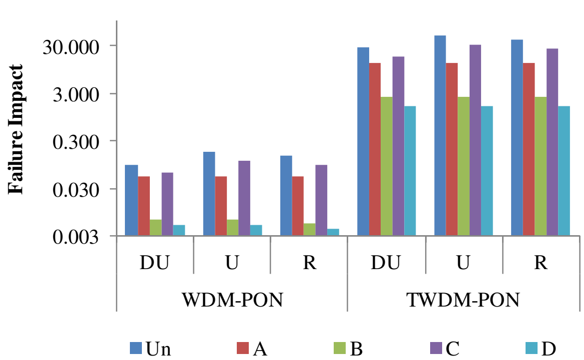


Fig. 5: Failure impact (FI) of different schemes for WDM- and TWDM-PON

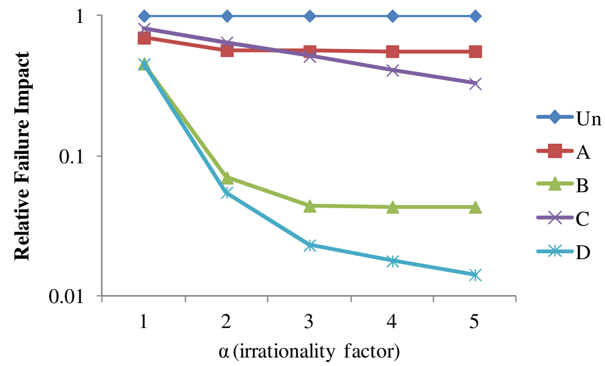


Fig. 6: Failure impact (FI) of different schemes for WDM-PON with varying α.

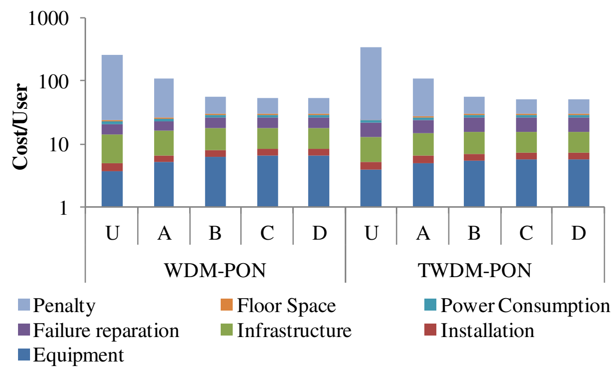


Fig. 7: Cost (total network cost divided by the total number of users) evaluation of various WDM- and TWDM-PON architectures.

REFERENCES

[1] Klaus Grobe et al., "Cost and energy consumption analysis of advanced WDM-PONs," IEEE Commun. Mag., vol. 49, no. 2, 2011, pp: s25-s32.

[2] A. Dixit, B. Lannoo, G. Das, D. Colle, M. Pickavet, and P. Demeester, “Flexible TDMA/WDMA Passive Optical Network: Energy Efficient Next-Generation Optical Access Solution,” OSN, vol. 10, no. 4, Nov. 2013, pp: 491-506, http://dx.doi.org/10.1016/j.osn.2013.03.001.

[3] Y. Luo et al., Time and Wavelength Division Multiplexed Passive Optical Network (TWDM-PON) for Next Generation PON Stage 2 (NG-PON2), Journal of Lightwave Technology 31 (4) (2013) 587 – 593.

[4] Business class services over a GPON Network, available at: http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/BusinessClass-GPON.pdf

[5] A. Dixit et al., “Efficient Protection Schemes for Hybrid WDM/TDM Passive Optical Networks,” *Workshop on New Trends in Optical Networks Survivability, IEEE ICC*, Ottawa, Canada, June 2012.

[6] A. Dixit, B. Lannoo, D. Colle, M. Pickavet, and P. Demeester, “Trade-off between End-to-End Reliable and Cost-Effective TDMA/WDM Passive Optical Networks,” Proc. RNDM 2012.

[7] M. Vogt, R. Martens, and T. Andvaag, “Availability modeling of services in IP networks”, *DRCN*, Banff, Canada, Oct. 2003.

[8] J. Kim, S. Yen, S. Fu, and L. G. Kazovsky, “Resilient optical access networks: optimization on the number of spikes in the StarRing”, *Workshop on Photonic Technologies for Access and Bio-Photonics*, Jan. 2011.

[9] M. Mahloo, A. Dixit, J. Chen, C. M. Machuca, B. Lannoo, D. Colle, L. Wosinska, “Towards Reliable Hybrid WDM/TDM Passive Optical Networks,” IEEE Commun. Mag., Feb. 2014.

[10] OASE Project, D4.2.1: Technical assessment and comparison of next-generation optical access system concepts, Oct. 2011.

[11] M. Mahloo, C. M. Machuca, J. Chen, and L. Wosinska, “Protection cost evaluation of WDM-based next generation optical access networks,” Optical Switching and Networking, vol. 10, no. 1, Jan. 2013, pp: 89-99.