Computer Networks xxx (2010) xxx–xxx

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A reliability analysis of Double-Ring topologies with Dual Attachment using *p*-cycles for optical metro networks

P.M. Santiago del Río [a], J.A. Hernández [a,*], J. Aracil [a], J.E. López de Vergara [a], J. Domżał [b], R. Wójcik [b], P. Chołda [b], K. Wajda [b], J.P. Fernández Palacios [c], Ó. González de Dios [c], R. Duque [c]

[a] *Universidad Autónoma de Madrid, C/ Francisco Tomás y Valiente 11, E-28049 Madrid, Spain*
[b] *AGH University of Science and Technology, Al. Mickiewicza 30, 30-059 Krakow, Poland*
[c] *Telefónica I+D, C/ Emilio Vargas 6, E-28943 Madrid, Spain*

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Network resilience
Availability
Survivability
Reliability
p-Cycles
DRDAs

ABSTRACT

The distribution of multicast traffic (e.g. IPTV or business point-to-multipoint) in the metropolitan environment requires highly resilient network infrastructures. Currently-deployed fibre ducts in the metropolitan area are typically based on ring topologies interconnected by the dual homing approach. In this study, an easy evolution towards meshed topologies is proposed, based on Double Rings with Dual Attachments (DRDA). This work analyses in detail the resilience capabilities of DRDAs and the two dual *p*-cycles defined over them. It is shown that, just by ensuring service repair rates of 12 h, large service availability values can be achieved (of the order of four to five-nines). Additionally, the amount of backup capacity required to recover from link failures is further calculated in this paper. Furthermore, this work gives a mathematical framework or reference to all those network operators who are willing to deploy highly resilient metropolitan area networks at a moderate cost. The five-nines service availability degree is easily achieved provided sufficiently small service repair times (in the range of 12 h). Additionally, large service availability values are obtained with little extra backup capacity (about three-nines with only doubling capacity).

1. Introduction

The research community is beginning to understand that only new optical network technologies can satisfy the ever-increasing user demands for bandwidth [1–3]. Indeed, recent experiments have shown line-rate capacities of up to Tbits/s with DWDM optical networks [4–6]. Once such bandwidth demands are satisfied with the help of optical switching, network operators must design resilience mechanisms on top of them to guarantee that end-users indeed perceive a substantial increase in the Quality of Service offered. Failure tolerance has become a priority to network operators during the design of their Metropolitan Area Networks.

Clearly, the perception by end-users of a 10-Gbps optical network might be better than that of a 100-Gbps optical network, provided that the former shows a greater degree of service availability than the latter. Network operators often seek to guarantee the so-called five-nines service availability of their networks. That is, the network is at the users' disposal at least during 99.999% of the time. This is in fact a very challenging issue given that both link and node failures occur more often than expected, leading to continuous service disruption. One link failure per year for every 450 km of fibre length is typically assumed by the research community as a reasonable value [7].

In IP-based packet networks, the routing protocols are capable of detecting link failures and distributing this information to all nodes within a domain such that, after some time, the routing tables in all nodes converge to the optimal solution. However, this process is very slow

* Corresponding author. Tel.: +34 91 624 8459; fax: +34 91 624 8749.
E-mail address: Jose.Hernandez@uam.es (J.A. Hernández).

1389-1286/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2009.10.018

and may take several seconds (even minutes), which is unacceptable for many delay-sensitive applications. It is feasible to reduce such delay by making use of the existing resilience techniques provided by the underlying optical layers.

In light of this, the research community has devoted great research effort to define mechanisms, algorithms, protocols and techniques over the control plane that improve and even guarantee service availability and survivability. These include, for instance, the classical 1 + 1, 1:1 and M:N protection techniques whereby two separated (often link-disjoint) paths, the so-called primary and backup paths, are used for the transmission of critical data.

For instance, Resilient Packet Rings (RPRs) [8] comprise a very promising 1:1 protection-based resilience mechanism for ring topologies, whereby link failures are guaranteed to recover within 50 ms. In RPRs, all links in the ring are full-duplex, allowing data the opposite direction when one link of the ring fails. A large number of studies have analysed the properties and benefits of RPRs, leading to the creation of the IEEE 802.17 Working Group on attempts to summarise its behaviour onto a common standard for Metropolitan 10 Gbit-Ethernet.

Over the past decade, an alternative to RPRs has been proposed via the so-called preconfigured protection cycles (also referred to as *p*-cycles) [9]. Such *p*-cycles have the advantages of common ring protection mechanisms (fast recovery time) and of meshed protection techniques (high capacity efficiency). Such fast path recovery is achieved since the backup path is preconfigured before the link failure actually occurs, just like RPRs. However, *p*-cycles are preferable over other preconfigured mechanisms such as RPRs given their high-redundancy structure and minimum extra capacity requirements per link.

Concerning *p*-cycles, the literature has: defined them [9], proposed a protocol for fast failure recovery [10] and probabilistically analysed their reliability properties [11], among many other studies [12–14]. This study goes one step further defining the emerging Double-Ring topologies with Dual Attachment (DRDAs) and studying the service availability and resilience properties of the two dual *p*-cycles defined over them. In such DRDAs, two different rings (the inner and the outer rings) are interconnected via dual attachments such that every node in the inner ring is double linked to its associated node in the outer ring to increase the redundancy and protection properties of the whole topology. Over such topologies, two disjoint *p*-cycles with no link shared between them provide protection to all nodes in the DRDA in case of failure, thus strengthening its survivability properties.

This work is devoted to the study of the service availability and design of such dual *p*-cycles on DRDA topologies. To this end, the remainder of this work is organised as follows: Section 2 gives a brief introduction to *p*-cycles and formally overview DRDAs. Section 3 presents a detailed study of the different combinations of link failures that may occur and provides the mathematical formulation of the problem under study. Additionally, this section studies the main availability metrics and minimum extra capacity required per link with a set of numerical examples. Section 4 proposes a set of experiments to numerically show the benefits of DRDAs and the dual *p*-cycles defined over them. Finally, Section 5 concludes this work with a brief summary of the main findings obtained.

2. Problem statement

2.1. Review of *p*-cycles

According to the seminal study made by the authors in [9], a preconfigured protection cycle (abbreviated as *p*-cycle) is defined as a set of links connected in a circular way such that all links in the *p*-cycle have *C* units of spare capacity that can be used to transport data in case of failure (Fig. 1-a left). Additionally, Ref. [9] defines two different types of failures that a *p*-cycle can recover from: the “on-cycle” span failure (Fig. 1-b middle) and the “straddling” span failure (Fig. 1-c right). The former case refers to a link that belongs to the *p*-cycle itself and can be recovered just by switching its traffic on the opposite direction of the *p*-cycle. The latter type of a failure refers to a link that does not belong to the *p*-cycle itself but can be recovered through it since the link’s edges are actually connected to two-nodes of the *p*-cycle. Thus, for a generic network topology, *p*-cycles provide protection not only to all its link members, but also to all those spans which are connected to them, bringing high-redundancy and great levels of protection.

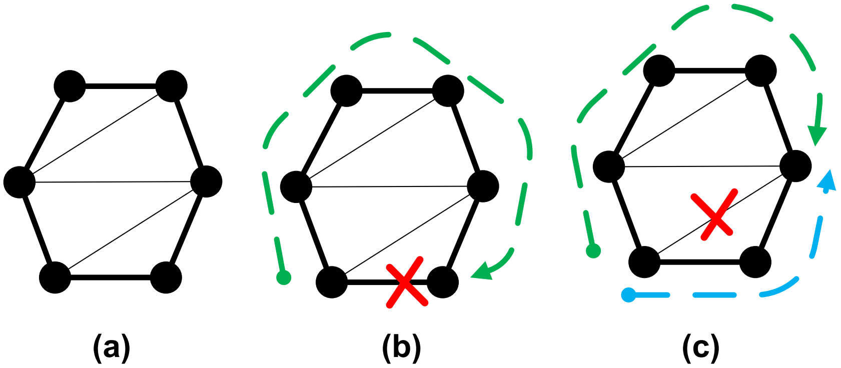


Fig. 1. Example of a *p*-cycle defined over a generic network topology. (a) The *p*-cycle itself; (b) an on-cycle link failure; and (c) a straddling link failure.

Designing p-cycles involves two stages: (1) deciding which links among the total comprise the p-cycle; and (2) defining the spare capacity units that all links on the p-cycle dedicate for failure provisioning. Concerning the latter, it is worth remarking that every straddling span failure consumes $C/2$ of extra capacity in a p-cycle, whereas on-cycle failures demand C units of protected capacity, as noted from Fig. 1. Additionally, a given p-cycle provides two separate paths for recovering from a straddling span failure.

The next section introduces Double-Ring topologies with Dual Attachment and the two dual p-cycles defined over them.

2.2. Definition of DRDAs and failure recovery

As formerly proposed in [15], a Double-Ring topology with Dual Attachment (DRDA in what follows) comprises two bi-directional rings of the same size (same number of links), one is called the inner ring and the other is referred to as the outer ring. Moreover, such double rings are interconnected in a way such that each node in the outer ring is attached with its associated node in the inner ring via a dual bi-directional link. The total number of nodes k in the DRDA topology determine the size and properties of the DRDA. For instance, Fig. 2 shows a DRDA with $k = 8$ nodes, therefore with $2k = 16$ links in it, each of them subject to faults. The reader will easily note that both the inner and outer rings must be of the same number of nodes and, such a number must be even, otherwise it is not possible to build the p-cycles (see Fig. 3).

As noted, the two dual p-cycles traverse all nodes in the topology providing full connectivity between any two-nodes in the DRDA. Also, the two p-cycles are link-disjoint, that is, no link is shared between them. These two features of DRDAs are expected to provide high levels of protection against link failures. In fact, such a redundancy level is observed from the fact that every link failure in the DRDA can be treated (and further recovered) as either an on-cycle failure on its actual p-cycle, or as a straddling span failure from the viewpoint of its dual p-cycle. Such resilience capabilities are studied in the next section.

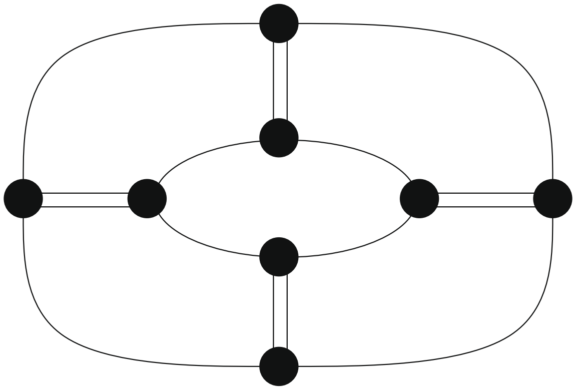


Fig. 2. Example of an 8-DRDA network topology.

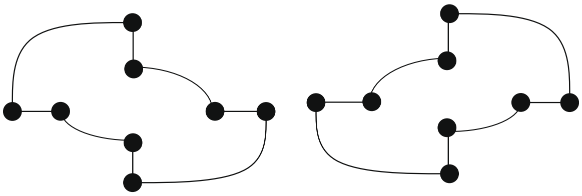


Fig. 3. The two p-cycles on an 8-DRDA network topology.

Before that, it is necessary to make clear that such two link-disjoint p-cycles require three very particular conditions to be met: (1) The metro network must be comprised of two bi-directional rings of the same number of nodes; (2) every node in the inner ring must be connected with its associated node in the outer ring via two links, and (3) the number of nodes in the inner and outer ring must be even. As long as these three conditions are met, it is always possible to define the two link-disjoint p-cycles.

3. Reliability analysis of dual p-cycles in DRDAs

This section is devoted to the study of the so-called all-terminal reliability of DRDAs, which is related to the probability to have all nodes interconnected in any possible way. In what follows, disconnection refers to the case where a given node is isolated from the rest since none of the two p-cycles can recover from the link failures that occurred. Finally, each link in the DRDA is assumed to carry, at most, C units of traffic under normal activity and link failures occur independently. The number of failures that a DRDA can recover from, and the amount of protection (backup) capacity required to do so is studied below.

3.1. Single failure recovery

This section considers three types of span failures which can be recovered by the two p-cycles: *full-straddling*, *semi-straddling* and *on-cycle* span failures. The two p-cycles are link-disjoint and, at the same time, traverse (thus protect) all nodes in the topology. For this reason, every link failure can be recovered by either its actual p-cycle (the p-cycle which contains the failing link) or its dual p-cycle (the other one, which does not contain the failing link but protects its connecting nodes), as explained below:

- *Full-straddling span failure (F–S)*: In this case, a span failure is recovered by the link's dual p-cycle, over the two different paths defined on it (see Fig. 4-a top). To recover the C units of capacity carried by the failing link, the two paths on the dual p-cycle are required to provide $C/2$ of protection capacity each.
- *Semi-straddling span failure (S–S)*: In this second case, a failure is recovered again by its dual p-cycle, but this time it is done by only the shortest path among the two possible ones defined by the p-cycle (see Fig. 4-b middle). This case requires the backup path defined over the p-cycle to have C units of extra capacity.
- *On-cycle span failure (O–C)*: In this final case, a span failure is recovered by its actual p-cycle, that is, by the same p-cycle which contains the link that happened to fail

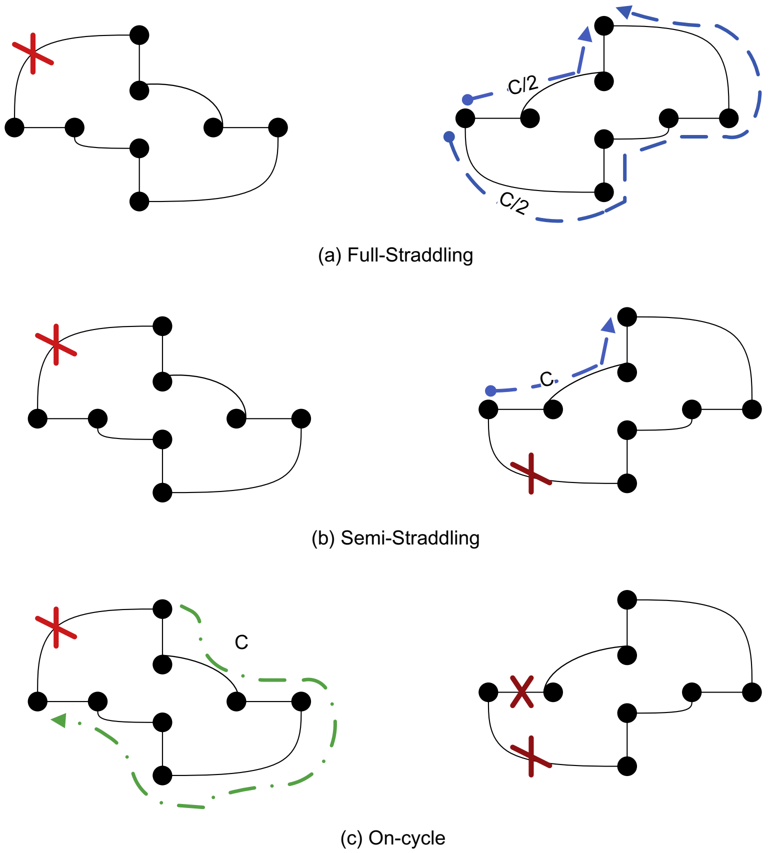


Fig. 4. The three possible strategies to recover from the failure on the figure's left-hand side *p*-cycle: full-straddling (top, a); semi-straddling (middle, b); and on-cycle (bottom, c).

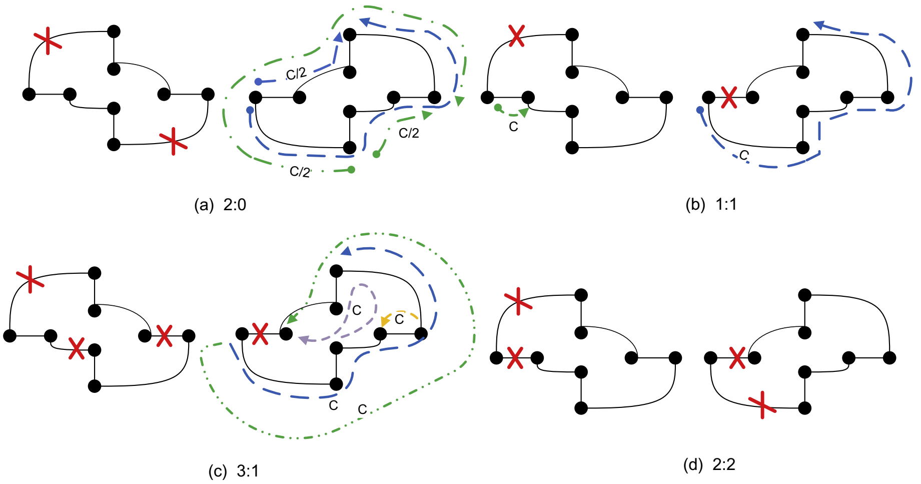
(see Fig. 4-c bottom). To recover from this failure, C units of extra capacity are required to transport the data on the opposite direction of the link's actual *p*-cycle.

In general, link failures can be recovered following any of the three strategies defined above. However, DRDAs should use the policy that requires the least amount of protection capacity, in order to provide spare capacity to recover from future link failures, if these ever happen to occur. Such a recovery policy depends on the actual number of failures and their location on the *p*-cycles at a given time. This is analysed next.

3.2. Multiple link failure recovery

Let $(n{:}m)$ denote the state in terms of the number of link failures of a k-DRDA topology at a given time. Here n and m refer to the number of link failures on the two *p*-cycles respectively defined in the k-node DRDA, with $0 \leqslant n, m \leqslant k$ since each *p*-cycle contains k links. The following lists all possible states concerning multiple link failures that may occur, along with the amount of spare capacity required for backup purposes C_b in order to ensure all-node connectivity:

- $(n{:}0)$: This state considers n span failures that occurred on one *p*-cycle, but no failures occurred on its dual *p*-cycle, where $1 \leqslant n \leqslant k$ (see Fig. 5-a top-left). All such failures on the same *p*-cycle are thus recovered on its dual *p*-cycle following a Full-Straddling strategy. This state thus consumes $C_b = nC/2$ of extra capacity on the dual *p*-cycle to recover from all failures.
- $(1{:}1)$: This state considers two link failures, one on each *p*-cycle. In this case, the two link failures are recovered on their dual *p*-cycles, following a Semi-Straddling strategy (see Fig. 5-b top-right). This state requires at least $C_b = C$ units of extra capacity on each *p*-cycle.
- $(n{:}1)$: In this state, one *p*-cycle has suffered n link failures, with $2 \leqslant n \leqslant k$, and its dual *p*-cycle only one link failure. Any failure on the first *p*-cycle can be recovered in its dual one by means of only one path, that is, following a Semi-Straddling recovery mechanism (see Fig. 5-c bottom-left). The single failure on the second *p*-cycle is recovered over it following an on-cycle policy. Therefore, this state may require an amount of backup capacity of, at least, $C_b = (n+1)C$ to recover from all link failures.
- $(m{:}n)$: When $m, n \geqslant 2$, this case leads to disconnection, that is, the all-terminal connectivity between any two pair of nodes is not guaranteed regardless of the amount



(a) 2:0

(b) 1:1

(c) 3:1

(d) 2:2

Fig. 5. Multiple link failure cases: state (2:0) (top-left, a); state (1:1) (top-right, b); state (3:1) (bottom-left, c) and state (2:2) (bottom-right, d).

of backup capacity provisioned (see Fig. 5-d bottom-right).

A summary of these cases, the amount of backup capacity required and the recovery strategy used in each case are given in Table 1.

As shown in Table 1, all cases of multiple link failures can be recovered just by defining the appropriate recovery policy with sufficient spare capacity. Only the state (*m:n*) with $m, n \geqslant 2$ brings a disconnection situation to the DRDA regardless of the amount of extra capacity provided by the two dual *p*-cycles.

It is worth noting that the amount of backup capacity required for each multiple link failure case shown in Table 1 refers to worst possible cases. For instance, some (*m:1*) failure cases may be solved with less than $C_b = (m+1)C$. However, in order to reduce the number of states and simplify the forthcoming Markov Chain analysis, Table 1 shows only the worst possible cases such that, if the value of C_b is guaranteed, then the strategy is capable of recovering from any particular failure combination of links for a given case. The next section studies the disconnection probability distribution making use of such a simplified Continuous Time Markov Chain (CTMC).

3.3. CTMC modelling and solution

The following analysis assumes that links in the DRDA happen to fail independently from one another. Additionally, link failures occur with a memoryless nature, that is, the inter-failure times are exponentially distributed with rate λ failures per unit of time. The value of λ^{-1} shall be referred to as the Mean Time Between Failures (MTBF). Also, links are assumed to be repaired by the network operator following again an exponential distribution with rate μ repaired links per unit of time. Now, μ^{-1} is referred to as the Mean Time To Repair (MTTR). The main goal of this study is to find the Time To Disconnection (TTD) probability distribution function of a generic *k*-DRDA topology and derive its Mean Time To Disconnection (MTTD) average value, given an observed average link failure value of MTBF and provided that the network operator can guarantee a certain average link repair time given by its MTTR value.

Table 1
Combinations of multiple link failures, recovery strategy and backup capacity required.

Failure case	Recovery strategy	Necessary C_b
(*n:0*) with $1 \leqslant n \leqslant k$	*n* F–S	$nC/2$
(*1:1*)	2S–S	C
(*m:1*) with $2 \leqslant m \leqslant k$	*m* S–S + 1 0–C	$(m+1)C$
(*m:n*) with $m, n \geqslant 2$	Not possible	Disconnection

To simplify the model, no more than four link failures are assumed to occur simultaneously. Indeed, the probability to have more than four link failures simultaneously is less than 10^{-6} for MTBF = 60 days and traditional MTTR values of hours and days.

With these assumptions, a given *k*-node DRDA can be easily characterised and analysed with the nine-state Reliability CTMC shown in Fig. 6, which reads as follows: The generic state (*m:n*) gives the number of failures on the two *p*-cycles, together with the required units of backup capacity C_b for that state. For instance, the state labeled (2:1) means that two of the *k* links of one *p*-cycle have failed together with one of the *k* links of its dual *p*-cycle. In such a case, 3*C* additional units of backup capacity are required.

The diagram in Fig. 6 also gives the transition probabilities between states. For instance, transition from state (0:0) to state (1:0) occurs with rate $2k\lambda$, since this transition occurs when any of the 2*k* links of the two *p*-cycles fails. Transition back to state (0:0) occurs with rate μ, which refers to the rate at which such a failure is fixed. For instance, transition from state (1:0) to state (1:1) occurs with rate $k\lambda$ (any of the *k* links of the dual *p*-cycle fails), whereas the transition rate to state (2:0) is $(k-1)\lambda$ (any of the $k-1$ remaining links of the current *p*-cycle fails). Again, transition back from state (2:1) to state (2:0) occurs with rate 1μ which refers to the fact that the

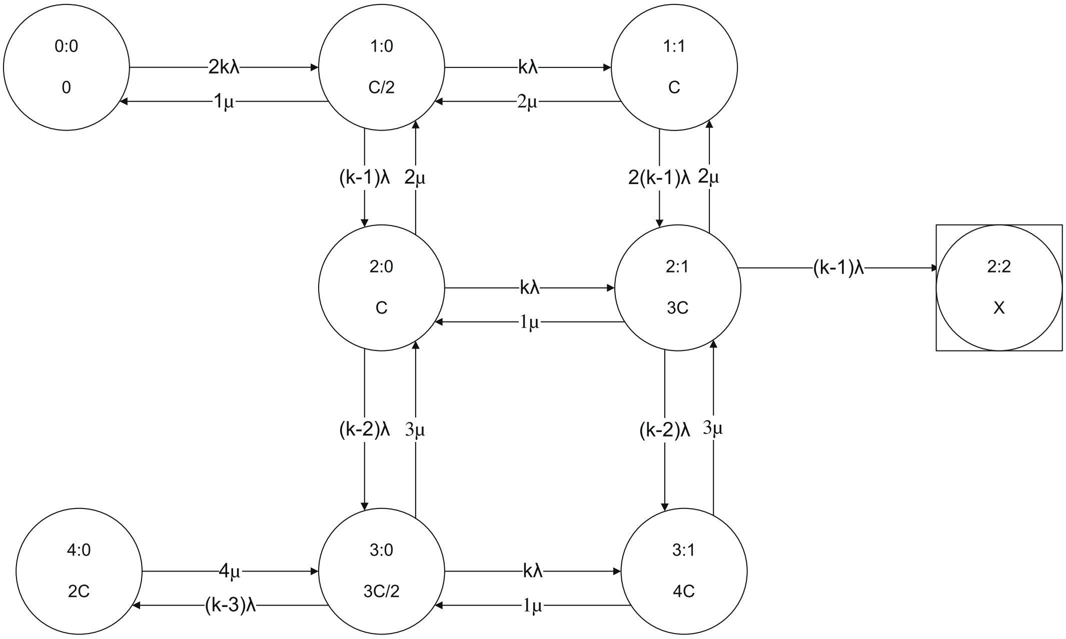


Fig. 6. The 9-state reliability Markov model for a generic *k*-DRDA.

Table 2
k-Node DRDA transition matrix *G*. The empty gaps refer to zeroes.

State	(0:0)	(1:0)	(1:1)	(2:0)	(2:1)	(3:0)	(4:0)	(3:1)	(2:2)
(0:0)	$-2k\lambda$	$2k\lambda$							
(1:0)	1μ	$-1\mu-(2k-1)\lambda$	$k\lambda$		$(k-1)\lambda$				
(1:1)		2μ	$-2\mu-2(k-1)\lambda$		$2(k-1)\lambda$				
(2:0)		2μ		$-2\mu-(2k-2)\lambda$	$k\lambda$	$(k-2)\lambda$			
(2:1)			2μ	1μ	$-3\mu-(2k-3)\lambda$			$(k-2)\lambda$	$(k-1)\lambda$
(3:0)				3μ		$-3\mu-(2k-3)\lambda$	$(k-3)\lambda$	$k\lambda$	
(4:0)						4μ	-4μ		
(3:1)					3μ	1μ		-4μ	
(2:2)									

failure on the dual *p*-cycle is recovered. The same reasoning applies to the rest of state transition rates. Finally, the state (2:2) is absorbing in the CTMC (there is no transition from this state to any other) and, when reached, this state implies that some nodes in the DRDA are isolated (disconnection state).

To compute the Time To Disconnection probability distribution from initial state (0:0), it is just required to choose the entry ((0:0),(2:2)) in the matrix $A(t) = e^{-Gt}$ where $A(t)$ gives the distribution function of the passage time between any two states of the CTMC within the time interval $[0, t]$, and matrix G is the transition probability matrix for this chain defined by Table 2.

The use of algebraic software, such as Derive or Mathematica, can be used to derive exact analytical expressions of the MTTD as a function of k, μ and λ.

Finally, Fig. 7 shows the Availability Markov model which is the same diagram as the Reliability Markov Model depicted in Fig. 6 but with state transition back from (2:2) to (2:1). This model makes it possible to compute the stationary probability distribution of all states, therefore, the amount of backup capacity required by the DRDA on average per unit of time, as shown throughout the experiments section.

Deriving such stationary probabilities of states requires solving the linear equation system (see [16], chapter 5 and [17], chapter 4):

$$\Pi_i q_i = \sum_{j \in S} q_{ij} \Pi_j \quad \text{for } i \in S, \tag{1}$$

$$\sum_{j \in S} \Pi_j = 1, \tag{2}$$

where Π_i is the stationary probability distribution of state i,S is the state space, q_{ij} is the transition probability from the state i to the state j and $q_i = \sum_{j \in S} q_{ji}$.

3.4. Recovery strategies

Concerning recovery strategies, the Availability Markov Model of Fig. 7 gives the amount of backup capacity required on each failure state, together with appropriate

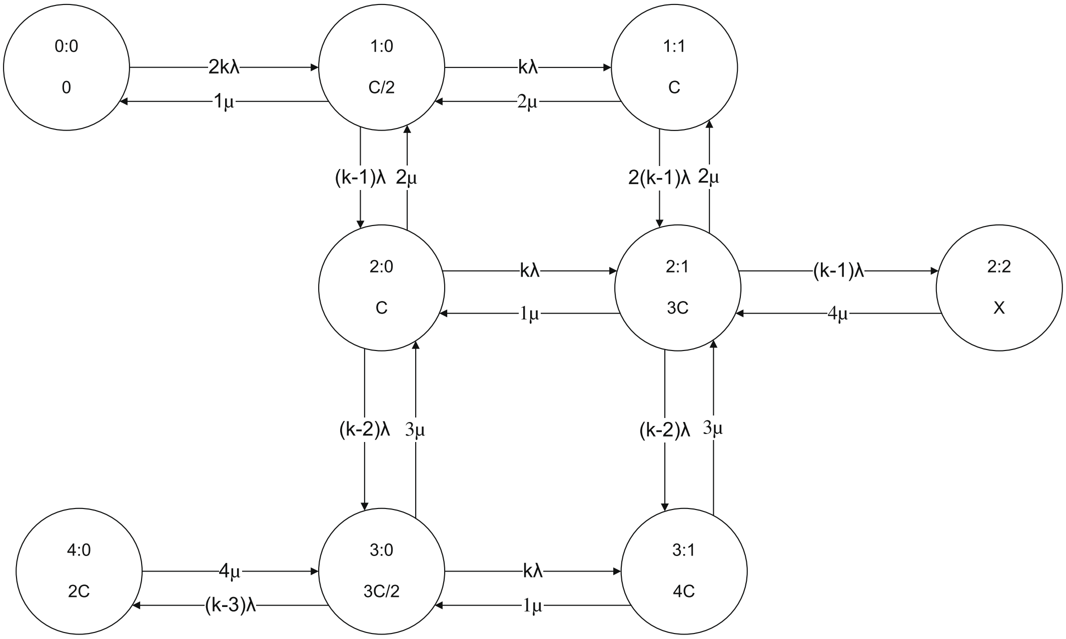


Fig. 7. The 9-state availability Markov model for a generic *k*-DRDA.

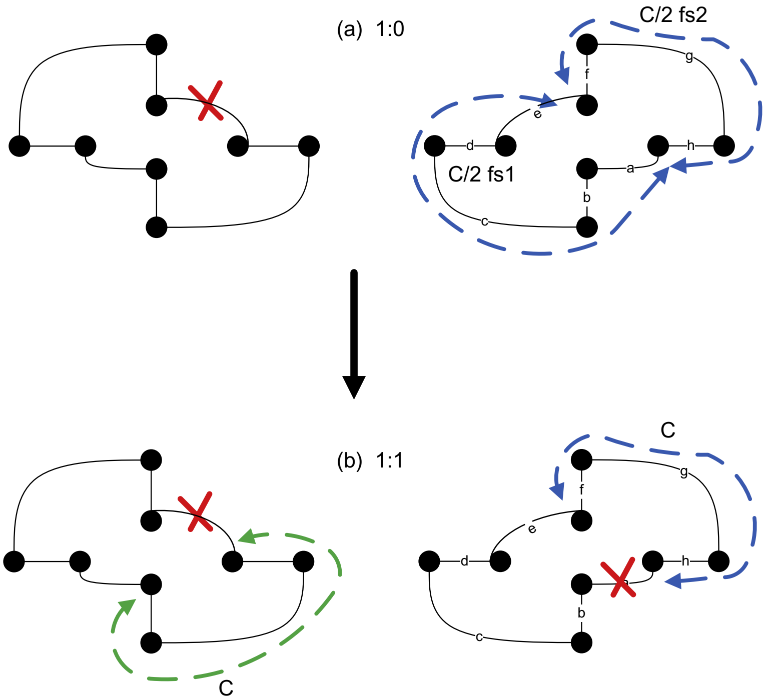


Fig. 8. Recovery strategy transition: State (1:0) (top, a); state (1:1) (bottom, b).

recovery policy that must be followed. For instance, starting on state (0:0), the first link failure is recovered with the Full-Straddling policy on its dual *p*-cycle. Subsequent link failures on the same *p*-cycle as the original failure are also recovered on the dual *p*-cycle following the Full-Straddling policy, since this is the cheapest solution (less amount of required backup capacity).

However, if a second link failure occurs on the dual *p*-cycle as the original failure, then the recovery strategy must switch to two Semi-Straddling recovery paths. Clearly, this seems to require re-configuration of the recovery policies since the original Full-Straddling path seems no longer necessary. However, as noted from Fig. 8, this is not the case: the original Full-Straddling path becomes a Semi-Straddling backup path, that is, it carries the total capacity of the two Full-Straddling paths, plus a new Semi-Straddling path needs to be created on the dual p-cycle to recover from the second link failure.

This obviously needs real-time re-configuration of protection strategies. Such reconfiguration must consider only two cases: The case of a second link failure on either $\{a,b,c,d,e\}$ (See Fig. 8) requires Full-Straddling fs_1 to divert its traffic to fs_2; and the case of a second link failure on either $\{f,g,h\}$ (See Fig. 8) requires Full-Straddling fs_2 to divert its traffic to fs_1. The re-configuration of such few cases can be calculated in the time between two link failures, provided that the time in between two consecutive link failures is sufficiently large. Indeed, the probability of having more than two link failures within one minute is less than 10^{-5} for MTBF $\geqslant$ 30 days.

The same reasoning applies to the case of switching from state (1:1) to state (2:1) which requires changing recovery policies from two S–S backup paths to two S–S and one O–C backup paths (see Table 1).

4. Numerical examples

This section provides a set of numerical examples to show the applicability of the equations derived in previous sections. Basically, these include the study of DRDA topologies with: (a) different MTBF and MTTR values, and (b) different topology sizes. Moreover, it is shown that a network operator must guarantee the appropriate MTTR in order to assure a given service-time availability for different observed MTBF values. Finally, it is studied how much backup capacity is necessary to provide in order for a network operator to guarantee a given service availability level.

4.1. Comparison for different MTBF and MTTR values

Fig. 9 shows the Time To Disconnection survival distribution function as a function of time (in days) assuming different MTBF and MTTR values. The values considered are: MTBF $= \{15, 30, 60, 180\}$ days, that is, one failure every 15 days, etc.; and average service repair times of MTTR $= \{1/4, 1/2, 1, 2, 7\}$ days. The worst possible case is that of failures occurring every 15 days and average service repair

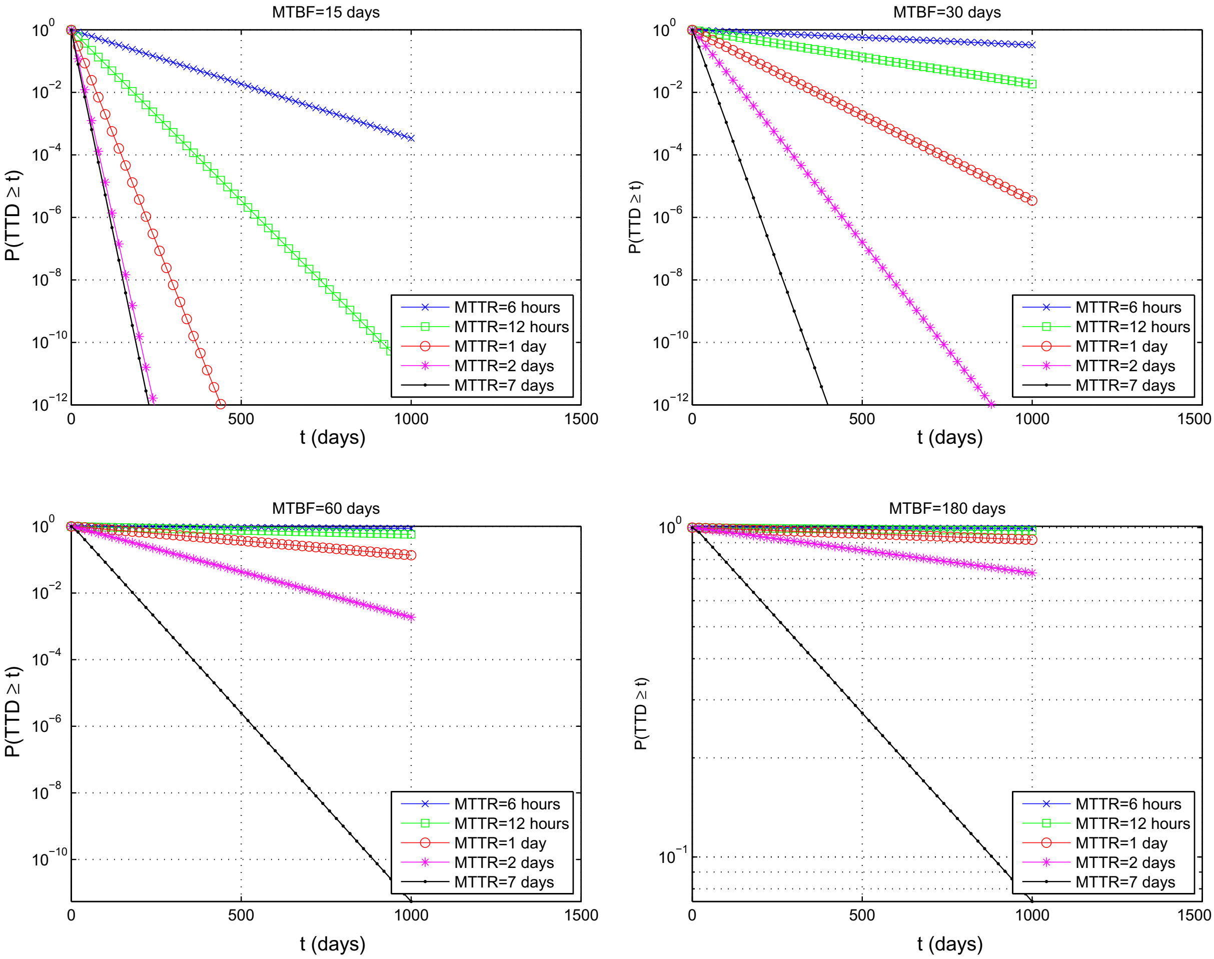


Fig. 9. Time to disconnection probability for different combinations of MTTR and MTBF.

time of 7 days. For instance, taking the value $t = 360$ days as a reference and service repair times of MTTR = 1 day, the probability to have the service available for more than $t = 360$ days (1 year) equals: 1.596×10^{-10} (almost impossible) when MTBF = 15 days, 0.011 when MTBF = 30 (one failure every month), 0.796 when MTBF = 90 and finally 0.970 when MTBF = 180.

Clearly, as can be seen from Fig. 9, the larger MTBF, the higher probability there is of one year of full-service availability.

4.2. Design of repair strategies

Concerning design purposes, it is important to find the MTTR that a network operator must ensure in order to guarantee a given disconnection probability over a period of time of one year (360 days), assuming the network has been observed to suffer one failure every MTBF. In light of this, Fig. 10 answers this question: it shows the probability to have disconnection over one month (30 days), over one half year (180 days) and over one year (360 days) considering MTBF = 60 days and different values of MTTR.

Fig. 11 shows the Mean Time To Disconnection (MTTD) for different MTTR and MTBF cases. The MTTD represents the average time required to move from the original (0:0) state with no link failures to the disconnection state in the Reliability Markov Chain. This gives an idea of what requirements (in terms of MTTR) that a network operator must demand from its service repair department in order to achieve a given MTTD. For instance, if a given DRDA is observed to suffer one failure every MTBF = 60 days, a department which fixes one failure within MTTR = 1/2 day (12 h) on average would give disconnection in MTTD = 1933 days on average, whereas if the same department guarantees MTTR = 1 day to fix a link failure, that would lead to MTTD = 577 days of MTTD.

In terms of service availability, Fig. 12 shows the *Service Time Unavailability* (STU), computed as:

$$STU = \Pi_{(2:2)}. \tag{3}$$

That is, STU represents the average proportion of time in which the network is not available. For instance, if a given DRDA is observed to suffer one failure every MTBF = 180 days and the network operator guarantees an average repair time MTTR in the range of 1 day or below, the target five-nines availability is provided.

Next section aims to compare the resilience capabilities of DRDAs in terms of its size.

4.3. Comparison between topology sizes

Fig. 13 shows the MTTD values for different k-size DRDAs. First of all, there is a decreasing trend of MTTD with respect to k since the more number of links (remark that a k-DRDA contains $2k$ links) in the topology, the more subject to failure this is. For instance, an 8-DRDA shows MTTD = 1933 days (MTBF = 60 days and MTTR = 1/2 day), whereas an 32-DRDA gives a much smaller MTTD = 35 days (less resilient).

Additionally, decreasing the MTTR has a clear impact on the MTTD, regardless of the topology size k, as shown in the previous case.

In conclusion, DRDAs are shown to provide high resilience capabilities, but these decrease with its size k (i.e. number of links subject to failures). The network operator

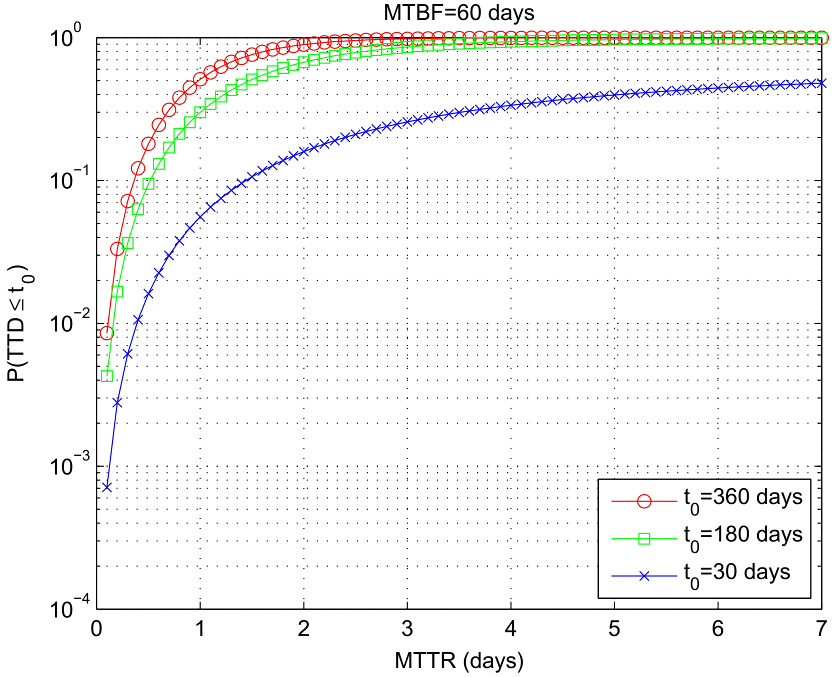


Fig. 10. Time to disconnection probability for different guaranteed MTTRs by the network operator.

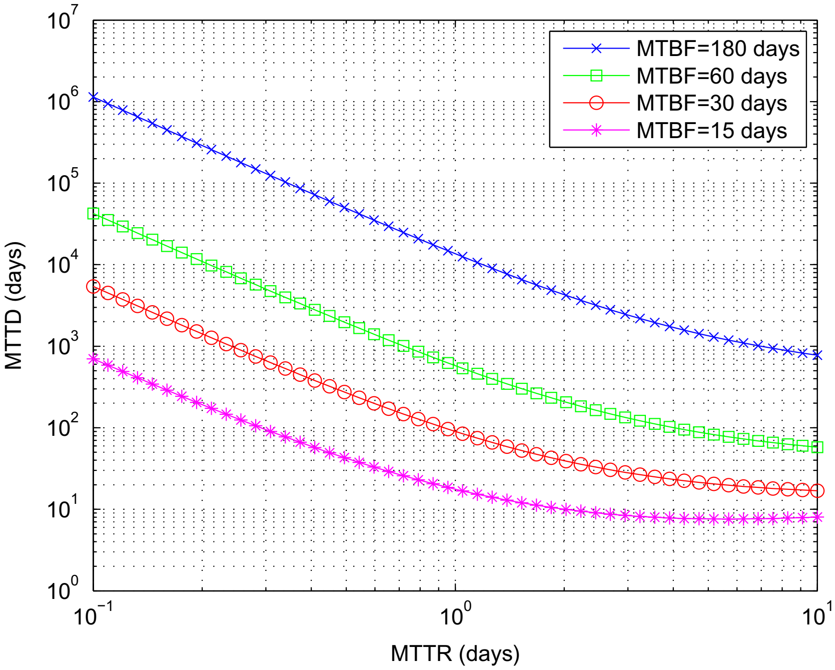


Fig. 11. Mean time to disconnection for different combinations of MTTR and MTBF.

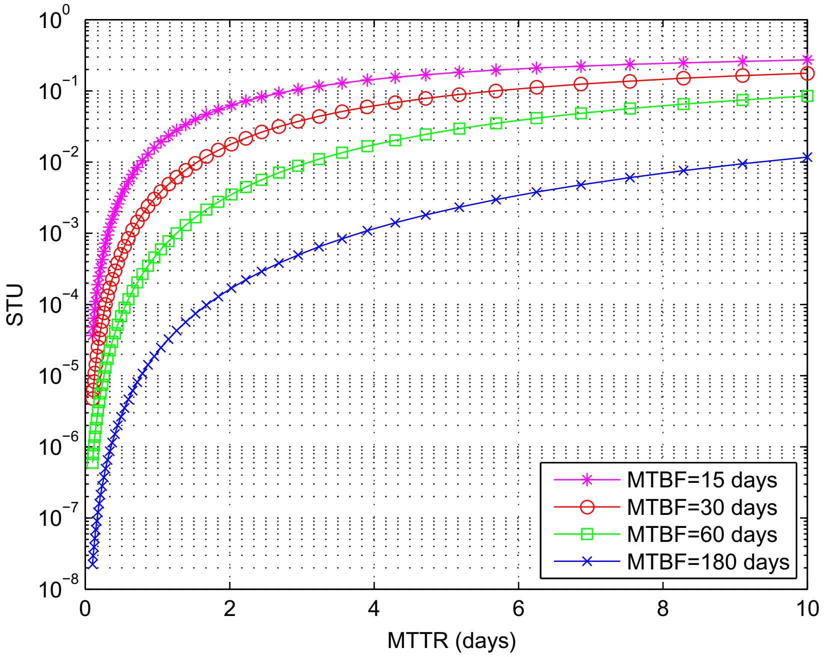


Fig. 12. Time service unavailability for different combinations of MTTR and MTBF.

must take care of this aspect when designing a given DRDA to cover a certain metropolitan area. Furthermore, when new nodes are included in the inner and outer rings to cover new neighbourhoods, the network operator must be aware that the total service availability gets reduced and must provide faster service repair times (reduce MTTR). This statement is confirmed in [11]. The *p*-cycles provide good resilience properties for MANs, but should not be used as a resilience mechanism for WANs, unless an outstanding MTTR value is guaranteed.

4.4. Network dimensioning

The next experiment aims to provide a means to provisioning backup capacity in the DRDA. As stated above, each failure state ((0:0), (*n*:0), etc) is recovered following a certain strategy (F–S, S–S, O–C) and such a recovery strategy demands a certain amount of backup capacity. For instance, $C/2$ extra/backup capacity is always required

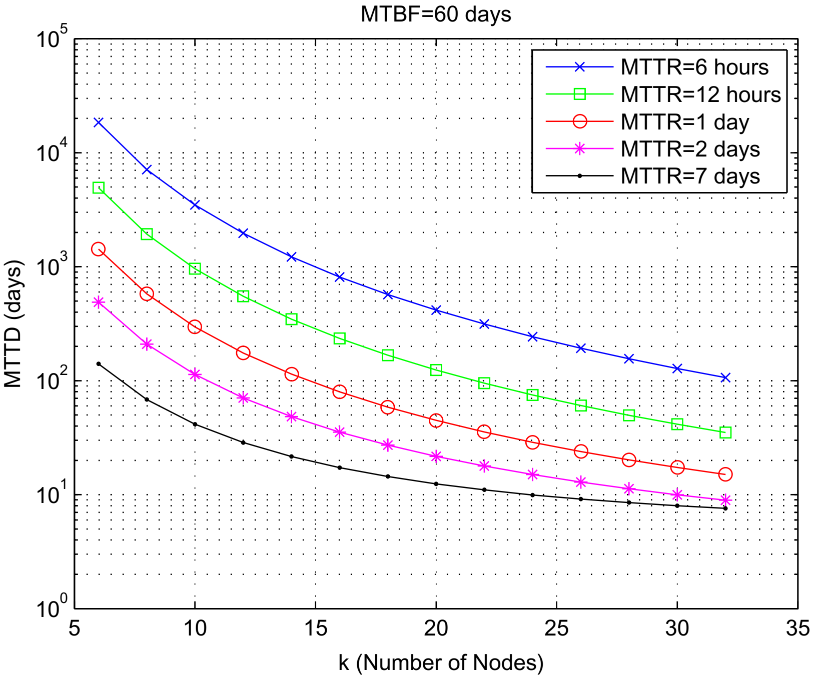


Fig. 13. Mean time to disconnection for different size of topology with different values of MTTR and MTBF = 60 days.

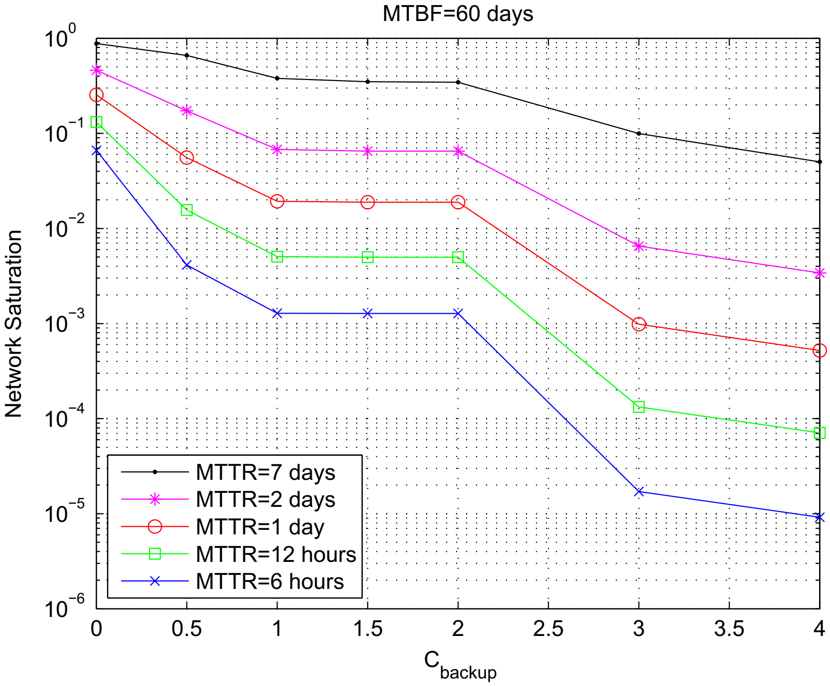


Fig. 14. Network saturation for different additional capacities with different values of MTTR and MTBF = 60 days.

Please cite this article in press as: P.M. Santiago del Río et al., A reliability analysis of Double-Ring topologies with Dual Attachment using *p*-cycles for optical metro networks, Comput. Netw. (2010), doi:10.1016/j.comnet.2009.10.018

whenever a single failure occurs (1:0) (see Fig. 7). However, $C/2$ backup capacity does not suffice if another failure occurs on either *p*-cycle. Such a case (states (1:1) and (2:0)) demands C units of backup capacity. Finally, other failure combination cases (or states) demand $3C/2, 2C, 3C$ and $4C$ of backup capacity for full-service recovery. No more than this quantity is required under the assumption of 4 link failures at most. Other than that is considered as disconnection.

Fig. 14 gives the stationary probability distribution of the cases that demand backup capacity: $C_b = \{0, C/2, C, 3C/2, 2C, 3C, 4C\}$. This gives an idea of the average portion of time over which the network is using such a capacity as backup. For instance, if only $C_b = 2C$ of backup capacity is provided, then there is network disconnection as soon as the states (2:1), (3:1) and (2:2) are reached, since there is not enough backup capacity to recover from such failures. Interestingly, $C_b = 1C$ provides service availability almost the same amount of time as if $C_b = 2C$, since the states (3:0) and (4:0), which require $C_b = 3C/2$ and $C_b = 2C$, respectively, occur more rarely than state (2:0) and (1:1) which require $C_b = C$. Essentially, the provisioning of too much extra backup capacity does not guarantee a much larger service availability level. There is a significant service availability improvement only if $C_b = 3C$ and $C_b = 4C$. For instance, assuming MTBF = 60 days and MTTR = 1/4 days (6 h), if the network operator guarantees an extra capacity of $C_b = 1C$, a saturation probability of 1.28×10^{-3} is obtained, whereas if $C_b = 4C$ is guaranteed, the five-nine service availability is provided (the saturation probability equals 9.17×10^{-6}).

5. Summary and conclusions

This work introduces Double-Ring topologies with Dual Attachment (DRDA) and studies their resilience capabilities against link failures. This topology comprises two bidirectional rings of the same size, namely the inner and the outer ring, whereby each node in the inner ring is connected with its associated node in the outer ring via dual-attachment, thus leading to a highly-redundant topology configuration. Such a solution is particularly useful when each pair of nodes (inner node and its dual attached outer node) are physically close, and the cost of connecting both nodes via dual-attachment is small. This is the case for most metropolitan area network of big cities.

Such resilience capabilities are modelled by a Continuous Time Markov Chain which, after solving, provides a useful insight in: (1) The repair times that a network operator must guarantee to achieve a given service availability; (2) the service availability provided by different size DRDA topologies and their implications in adding new nodes in the inner and outer rings; and, (3) the service availability provided with respect to the amount of backup capacity dedicated to recover from failures.

For instance, in order to achieve the five-nines service availability level (99.999% of the time) it is necessary to provide MTTR smaller than twelve hour to provide for typical MTBF values in the range of 15–60 days. For the same values, only the provisioning of $C_b = C$ backup capacity gives service unavailability of 10^{-3}, whereas $C_b = 4C$ guarantees the five-nine service availability. Easy rules like these can be obtained from the CTMC model and the figures depicted in the numerical examples.

This information is of special interest to provide multicast services which demand full-time any-to-any connectivity, such as the distribution of IPTV services. In such applications, a root node serves IPTV content to all other nodes in the topology, which further distribute this signal to a number of DSLAMs connected with it. In such a case, the isolation of a single node translates to thousands of users without IPTV service, which is unacceptable for most network operators.

Acknowledgments

The work described in this paper was carried out with the support of the BONE project ("Building the Future Optical Network in Europe"), a Network of Excellence funded by the European Commission through the 7th ICT-Framework Programme. This work was also supported by the Polish Ministry of Science and Higher Education under grant N517 013 32/2131.

The authors would like to express their gratitude towards Prof. Andrzej Jajszczyk for his valuable insights which helped to write this article.

References

[1] S. Yao, S.J.B. Yoo, B. Mukherjee, S. Dixit, All-optical packet switching for metropolitan area networks, IEEE Commun. Mag. 39 (3) (2001) 142–148.

[2] A. Jourdan, D. Chiaroni, E. Dorato, G.J. Eilenberger, F. Masetti, M. Renaud, The perspective of optical packet switching in IP dominant backbone and metropolitan networks, IEEE Commun. Mag. 39 (3) (2001) 136–141.

[3] J. Finochietto, J. Aracil, A. Ferreiro, J.P. Fernández-Palacios, O. González de Dios, Migration strategies towards all optical metropolitan access rings, IEEE/OSA J. Lightwave Technol. 25 (8) (2007) 1918–1930.

[4] Y. Miyamoto, K. Yonenaga, A. Hirano, N. Shimizu, M. Yoneyama, H. Takara, K. Noguchi, K. Tsuzuki, 1.04-Tbit/s DWDM transmission experiment based on alternate-polarization 80-Gbit/s OTDM signals, in: Proceedings of the European Conference on Optical Communication, vol. 3, 1998, pp. 53–57.

[5] S. Verma, H. Chaskar, R. Ravikanth, Optical burst switching: a viable solution for Terabit IP backbone, IEEE Network (2000) 48–53 (Nov.–Dec.).

[6] J. Yu, M.-F. Huang, Y. Shao, T. Wang, P. Magill, M. Cvijetic, L. Nelson, M. Birk, G. Zhang, S.Y. Ten, H.B. Matthew, S.K. Mishra, 32Tb/s (320 × 114 Gb/s) PDM-RZ-8QAM transmission over 580km of SMF-28 ultra-low-loss fiber, in: Proceedings of the Optical Fiber Communication Conference and Exposition National Fiber Optic Engineers Conference (OFC/NFOEC), San Diego, CA, USA, 2009.

[7] S.D. Maesschalck, D. Colle, I. Lievens, M. Pickavet, P. Demeester, C. Mauz, M. Jaeger, R. Inkret, B. Mikac, J. Derkacz, Pan-european optical transport networks: an availability-based comparison, Photon. Network Commun. 5 (3) (2003) 223–225.

[8] J. Domzal, K. Wajda, S. Spadaro, J. Solé-Pareta, D. Careglio, Recovery, fairness and congestion control mechanisms in RPR networks, in: 12th Polish Teletraffic Symposium (PSRT), Poznan, Poland, 2005.

[9] W. Grover, D. Stamatelakis, Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration, in: Procedings of the IEEE International Conference Communications (ICC'98), 1998, pp. 537–543.

[10] D. Schupke, Automatic protection switching for p-cycles in WDM networks, Opt. Switching Networking (OSN) 2 (1) (2005) 35–48.

[11] P. Cholda, A. Jajszczyk, Reliability assessment of optical *p*-cycles, IEEE/ACM Trans. Networking 15 (6) (2007) 1579–1592.

[12] H. Drid, B. Cousin, S. Lahoud, M. Molnar, Multi-criteria *p*-cycle network design, in: 33rd IEEE Conference on Local Computer Networks.

[13] M. Clouqueur, W.D. Grover, Availability analysis and enhanced availability design in *p*-cycle-based networks, Photon. Networking Commun. 10 (1) (2005) 55–71.

[14] G. Shen, W.D. Grover, Extending the *p*-cycle concept to path segment protection for span and node failure recovery, IEEE J. Select. Areas Commun. 21 (8) (2003) 1306–1319.

[15] A. Ferreiro, J. Derkacz, F. Dorgeuille, R. Huelsermann, M. Quagliotti, S. Verbrugge, Techno-economic benchmarking of NOBEL solutions for end-to-end broadband communications, in: Proceedings of the 12th European Conference on Networks and Optical Communications (NOC'07), Stockolm, Sweeden, 2007, pp. 352–359.

[16] S.M. Ross, Stochastic Processes, Wiley Series in Probability and Mathematical Statistics, second ed., John Wiley and Sons, 1996.

[17] O.C. Ibe, Markov Processes for Stochastic Modeling, Elsevier Science and Technology Books, Academic Press, 2009.

Pedro María Santiago del Río received the M.Sc. degree in Mathematics and Computer Science from Universidad Autónoma de Madrid in 2008. Before that, he joined the Networking Research Group at the Computer Science Department of UAM, where he has been participating in several European Union research projects (e-Photon One plus, BONE, OneLab2) and in the national research project DIOR. In 2009, he was awarded with a four-year fellowship by the Ministry of Education of Spain (F.P.U scholarship). His research interests are focused on the analysis of network traffic, optical networks, mathematical modeling, performance evaluation of communications networks, probability theory and statistics.

José Alberto Hernández completed the five-year degree in Telecommunications Engineering at Universidad Carlos III de Madrid (Madrid, Spain) in 2002, and the Ph.D. degree in Computer Science at Loughborough University (Leics, United Kingdom) in 2005. After this, he joined the Networking Research Group at Universidad Autónoma de Madrid (Spain), where he actively participates in a number of both national and european research projects concerning the modeling and performance evaluation of communication networks, and particularly the optical burst switching technology. His research interests include the areas at which mathematical modeling and computer networks overlap.

Javier Aracil received the M.Sc. and Ph.D. degrees (Honors) from Technical University of Madrid in 1993 and 1995, both in Telecommunications Engineering. In 1995 he was awarded with a Fulbright scholarship and was appointed as a Postdoctoral Researcher of the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley. In 1998 he was a research scholar at the Center for Advanced Telecommunications, Systems and Services of The University of Texas at Dallas. He has been an associate professor for University of Cantabria and Public University of Navarra and he is currently a full professor at Universidad Autónoma de Madrid, Madrid, Spain. His research interest are in optical networks and performance evaluation of communication networks. He has authored more than 50 papers in international conferences and journals.

Jorge E. López de Vergara (jorge.lopez_vergara@uam.es) is currently an associate professor in the Computer Science Department of the Universidad Autónoma de Madrid. He received his M.Sc. degree in telecommunications from the Technical University of Madrid in 1998 and finished his Ph.D. in telematics engineering at the same university in 2003, where he held a research grant. He has participated in several Spanish and EU research projects, and has authored more than 50 papers in international conferences and journals. His current research topics include network and service management and monitoring.

Jerzy Domżał received the M.Sc. and Ph.D. degrees in Telecommunications from AGH University of Science and Technology, Krakw, Poland in 2003 and 2009, respectively. Now, he continues his work at Department of Telecommunications at AGH University of Science and Technology. He is especially interested in optical networks and services for future Internet. He is involved in EU Projects: SmoothIT, BONE and EuroNF. He is a co-author of many technical papers.

Robert Wójcik received the M.S. degree in telecommunications from AGH University of Science and Technology, Kraków, Poland in 2006. Now, he is a Ph.D. student at AGH University. He is the co-author of 8 technical papers. He is involved in several international scientific projects: SmoothIT, NoE BONE and Euro-NF. His research interests focus on Quality of Service, Flow-Aware Networking and Overlay networks.

Piotr Chołda received a Ph.D. degree in Telecommunications from AGH University of Science and Technology, Kraków, Poland in 2006, which he joined the same year. His research interests focus on design of resilient multilayer networks as well as reliability modeling, including overlay networking. He is the co-author of five refereed journal papers and two tutorials on resilient networks. He is the recipient of the Communications QoS, Reliability and Performance Modeling Symposium Best Paper Award from ICC'06. Now, he is involved in two EU projects, Euro-NF and SmoothIT.

Krzysztof Wajda received his M.Sc. In Telecommunications from UKR in 1982 and Ph. D. (thesis title): Adaptive routing rules in circuit-Switched networks with SPC exchanges) in 1990. In 1982 he joined UKR where he was responsible for laboratory of switching technology. During period 1991–1993 he was granted a Monbusho (Japanese Ministry of Education) scholarship in Osaka University and Kyoto University. In 1996 he spent 6 months of sabbatical leave in CNET (France) working on Adaptive Connection Admission Control (CAC) in ATM networks. He was involved in few international projects: COST 242, Copernicus ISMAN, ACTS 038 BBL, TEMPUS JEP No. 0971 and was granted TEMPUS individual grant IMG-96-PL-2057. Currently he is involved in two international projects: FP6-506760 NOBEL and FP6-2002-IST-1/001933 ePhoton/One. He participated also in a few grants supported by National Science Foundation (in 2 was involved as a project leader). He serves also as a reviewer of few journals: elecommunications Systems, Performance Evaluation, Computer Networks and ISDN Systems and international conferences. He has been a consultant to private telecommunication companies and Polish Telecom. Main research interests: traffic management for broadband networks, multimedia services, architecture and implementation of ATM networks, performance evaluations of fast packet networks, internetworking. Dr Wajda is the author (or coauthor) of 5 books (in Polish) and over 70 technical papers.

Juan Pedro Fernández-Palacios Giménez. He graduated with a degree of Telecommunications Engineering from Polytechnic University of Valencia where he carried out his final project working on the simulation of wavelength converters. In September of 2000 he joined TIDSA where he has been working on the analysis and evaluation of optical technologies, likewise he has participated in European projects such as Eurescom P1014 TWIN and IST projects (DAVID, NOBEL, etc.) as well as other internal projects related to the development of optical networks in the Telefónica Group. Currently, he is Project Manager in the Division of Network Planning and Techno-Economic Evaluation of TIDSA.

Óscar González de Dios received his Masters Degree from the University of Valladolid in 2000 in Telecommunications Engineering. In 2000 he joined Telefónica I+D, where he worked for several years in the development and testing of telephony applications and interactive voice-response platforms. In 2005 he joined the Advanced Network Planning department in Telefónica I+D , where he has been working in the analysis and performance evaluation of optical networks. He has participated several R+D European projects, like IST NOBEL (I and II), e-Photon/One+, BONE and AGAVE. He has coordinated the CELTIC project BANITS 2. He is currently involved in internal innovation projects for the Telefónica group regarding optical network planning and optical network analysis.

Raúl Duque completed the five-year degree in Telecommunications Engineering at Universidad Carlos III de Madrid (Madrid, Spain) in 2007. In 2006, he joined the New Network Technologies Division at Telefónica I+D where he developed his degree dissertation about a new network resource management mechanism based on the Nominal Route concept. He is currently working in the Photonic Network Division at Telefónica I = D, where he is participating in internal research projects for the Telefónica group. His research interests include network performance, optical network planning, resilience techniques, multicast transport algorithms for IPTV and access control strategies.

Please cite this article in press as: P.M. Santiago del Río et al., A reliability analysis of Double-Ring topologies with Dual Attachment using *p*-cycles for optical metro networks, Comput. Netw. (2010), doi:10.1016/j.comnet.2009.10.018