RESEARCH ARTICLE

p-Cycle configuration possibilities over DRDA networks

Jerzy Domżał[1]*, Robert Wójcik[1], Andrzej Jajszczyk[1], Pedro M. Santiago del Río[2], José Alberto Hernández[3] and Javier Aracil[2]

[1] AGH University of Science and Technology, Department of Telecommunications, Al. Mickiewicza 30, 30-059 Kraków, Poland
[2] Universidad Autónoma de Madrid, Dept. Ingeniería Informática, Calle Francisco Tomás y Valiente, 11 - Madrid, Spain
[3] Universidad Carlos III de Madrid, Dept. Ingeniería Telemática, Avda. de la Universidad, 30 - E-28911 Leganés, Madrid (Spain)

ABSTRACT

A resilience analysis of protection cycles (*p*-cycle) configurations for *Double Rings with Dual Attachment* (DRDAs) architectures is presented in this work. DRDAs are composed of two rings with corresponding nodes connected by two separated links. There are several possible configurations of *p*-cycles, which may be used in DRDAs for improving link or node protection upon link failure. The values of the parameters *Mean Time To Failure* and *Mean Time To Disconnection* are analysed in the paper to show the best choice of *p*-cycles in DRDAs architectures. Copyright © 2014 John Wiley & Sons, Ltd.

*Correspondence

J. Domżał, AGH University of Science and Technology, Department of Telecommunications, Al. Mickiewicza 30, 30-059 Kraków, Poland.
E-mail: jdomzal@kt.agh.edu.pl

1. INTRODUCTION

New optical networking technologies have been more and more popular in recent years. They can satisfy still increasing user demands for bandwidth [1] but also have to be resilient and ensure quality of service for high priority connections. There are at least a few well-known solutions that ensure continuous data transmission in a network even in the case of link or node failures. For instance, Institute of Electrical and Electronics Engineers 802.17 standard defines *Resilient Packet Rings* (RPR) networks [2]. In RPR, data transmission is realised in both rings simultaneously, however, in opposite directions. When a failure occurs in the network, one of two protection mechanisms, that is, steering (mandatory) or wrapping (optional) is activated. In the first one, data is redirected to the opposite ring in the source node, whereas, in the second case, packets are wrapped to the opposite ring in the node situated next to the failed element. Because of the topology discovery protocol, which informs the nodes about the current network topology, it is possible to ensure data transmission with outages shorter than 50 ms, which is acceptable by most applications.

In this paper, we focus on the preconfigured protection cycles (*p*-cycles). They were proposed in 1998 as a powerful resilience technique to protect metropolitan area networks (MANs) against link or node failures [3]. Numerous past studies show the usefulness and advantages of this solution. The practical proposals, as well as theoretical analyses, have been provided to explain how this very promising approach performs. Most researchers use the (*Integer Linear Programming* model to find the best *p*-cycle configurations in a network, for example, in [4] and [5]. This simple and effective tool sometimes is used to solve very complex problems. Many new proposals regarding *p*-cycles have been identified in a literature. The *Failure Independent Path-Protecting p*-cycle that is an extension of the original concept is presented in [6]. This solution allows for more capacity efficient network design than the link protecting *p*-cycle. The recent work presented in [7] assumes that the combination of network coding and *p*-cycles ensures an effective $1 + N$ protection against single-link failures. The authors in [8] prove that protection by establishing optimised explicit paths allows for more effective balance of traffic in comparison to the use of optimised Internet Protocol (IP) routing. In [9], the schemes for Multiprotocol Label Switching networks that combine *p*-cycle and the fast reroute mechanisms are proposed to share the protection bandwidth effectively. The authors in [10] analysed a multipath protection algorithm based on the *p*-cycle mechanism. The obtained results confirm that this solution is more efficient than the path-based

protection concept. However, in [11], the authors propose a new path-based multipath protection scheme to control the lengths of paths, which allows for more effective transmission in a network. The paths may also be established effectively by using the mixed shared protection algorithm proposed in [12]. There are also many papers in which authors analyse the possible advantages of *p*-cycles when two or even more failures occur in a network. The simple solution is presented in [13], where two link-disjoint backup paths are computed for each link. As a result, the network is protected against two-link failures. The authors in [14] and [15] focus on the capacity optimization in a network with *p*-cycles when two failures are identified. In [16], the enhanced intelligent *p*-cycle is proposed to protect all working light-trees of multicast demands in a network. The *Quality Of Protection* for networks with *p*-cycles is analysed in [17]. The authors propose five service classes to protect links against failures. The best one, platinum class, ensures protection of all two-link failures. The *p*-cycles that ensure a network survivability when many (more than two) links fail have been also analysed, for example, in [18]. In the paper, a few new algorithms have been proposed to determine the number of disjoint *p*-cycles in the network with the same number of non-working links. In [19], the authors consider single and multiple failures and propose the new algorithms, which minimise the capacity consumption in a network protected by *p*-cycles. The authors of [20] also try to optimise the process of *p*-cycles selection. They use the integer linear programming and genetic algorithm methods to find the best solutions. The reliability analysis provides a key metric for choosing the best configuration of *p*-cycles in a given network topology [21].

There are two types of link spans protected by *p*-cycles, on-cycle and straddling ones (Figure 1). In the first case, the failing link is a part of a *p*-cycle. The failure is recovered by redirecting the transmission through the working spans, which belong to the *p*-cycle. In the second case, the failing link does not belong to the *p*-cycle, but transmission may be continued by using the spans that belong to the *p*-cycle. Moreover, in this case, it is possible to set two routes for redirected traffic, which demonstrates one of the greatest advantages of *p*-cycles. Additionally, the proposed method is fast due to its local character of protection switching.

In this paper, we propose an analytical model that facilitates the selection of an appropriate *p*-cycle configuration in the *Double Ring with Dual Attachment* (DRDA) network

architecture. Although we focus on DRDAs, the presented method may be easily extended for any other architecture. DRDAs are composed of two rings (the inner and the outer ring) interconnected via dual attachments, that is, each node in the inner ring is double linked to its associated node in the outer ring. DRDAs were introduced in [22], whereas, this paper presents the analytical comparison between various *p*-cycle configurations, for the first time. We provide the reliability analysis for five *p*-cycle configurations and prove that the one that was proposed and analysed in [22] has the best properties. Moreover, we show that this solution should be applicable only for smaller networks, for example, MANs. In wide area networks, more smaller *p*-cycle configurations ought to be considered.

Research on DRDA topologies is an important open topic because many network operators, such as Telefonica, are currently considering using DRDAs in their MANs. This interest comes from the fact that it used to be common to design MANs in a form of one or more rings. When such topology exists, it is easy to connect two rings with dual attachments and create a DRDA network. The research work on DRDA networks was conducted as a part of the BONE project funded by the European Commission under the 7th Frame Programme. One of the partners in this work was Telefonica. Currently, the work on DRDAs is continued in the TIGER2 project, also with researchers from Telefonica [23].

Over DRDA topologies, *p*-cycles may effectively provide protection in case of failure, thus strengthening its survivability properties. The number of nodes in a DRDA network must be divisible by four to allow for establishing the forthcoming *p*-cycle configurations under study. Five configurations of *p*-cycles are considered in the paper and their effectiveness is compared by means of a reliability analysis. The values of the following two metrics are derived, *Mean Time To Failure* (MTTF) and *Mean Time To Disconnection* (MTTD). Span repairs are not considered in the first one, while the second represents the mean time to achieve a disconnection state, when the connectivity cannot be guaranteed even though the failed spans are repaired with certain MTTR (*Mean Time To Repair*).

This paper is organised as follows. Five possible *p*-cycle configurations for DRDAs are proposed in Section 2. Sections 3.1 and 3.2 provide the analysis of MTTF and MTTD for each *p*-cycle proposal considered in the paper, respectively. In Section 3.3, capacity requirements for each
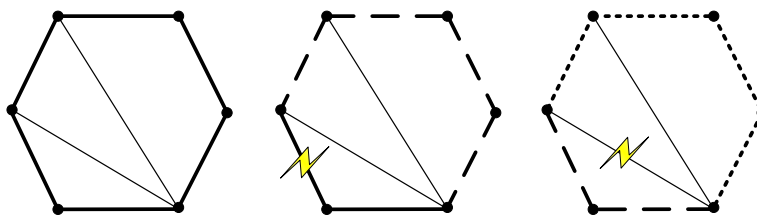

Figure 1. Example of *p*-cycles. (a) The *p*-cycle itself, (b) an on-cycle link failure and (c) a straddling link failure.
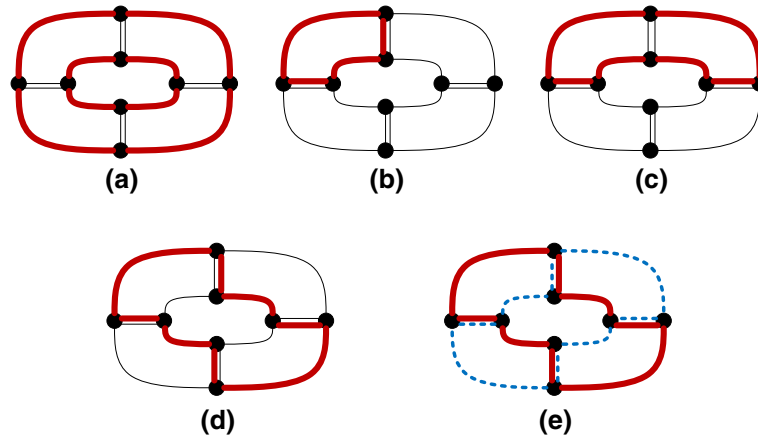
Figure 2. Evaluated *p*-cycle configurations.

p-cycle configuration are presented. Finally, Section 4 concludes the paper.

2. ANALYSED *P*-CYCLE CONFIGURATIONS

A *k*-node DRDA network (with 2*k* links) can be protected against link failures by several *p*-cycle configurations, as shown in Figure 2. It presents five possibilities that are analysed and compared in this paper. In case (a), a simple configuration is considered: two *p*-cycles, which cover the inner and the outer ring. Figure 2(b) proposes a different approach, that is, many (*k*/2) short (4-links) *p*-cycles (for simplicity, only one *p*-cycle is presented in this case). In case (c), there are two *p*-cycles, each spanning over the half of the network. Case (d) shows two *p*-cycles, both spanning through all the nodes in the network (again, only one is marked). As there is no information exchange between the *p*-cycles, each link failure is treated as an on-cycle failure and is repaired by the *p*-cycle to which this link belongs.

The last approach, Figure 2(e), presents the solution introduced in [22], where there are two cooperating *p*-cycles. The cooperation means that failures can be repaired either in the *p*-cycle in which a failure occurs, or in the complementary *p*-cycle, depending on which strategy is more efficient. The cooperation is possible, due to two features. Firstly, each *p*-cycle traverses all nodes in the topology providing full connectivity between any two nodes in the DRDA. Secondly, *p*-cycles are link disjoint. The presented features of *p*-cycles proposed in case (e) provide a high level of protection against link failures.

In cases (a) and (c), the established *p*-cycles do not cover all the links. k links in case (a) are not protected. In case (c), k-4 are straddling links protected by *p*-cycles. It is expected that in terms of reliability, these configurations will be inferior compared to the other cases; however, we decided to include them for the purpose of comparison and a better overall view. Similarly, all the proposed configurations differ in the amount of spare capacity that is required to provide full protection. Nevertheless, in this paper, we

focus mainly on the solutions' effectiveness rather than on their deployment costs.

3. ANALYSIS OF RELIABILITY AND REQUIREMENTS FOR DRDA NETWORKS WITH VARIOUS *P*-CYCLE CONFIGURATIONS

In this section, we compare the proposed *p*-cycle configurations in terms of achieved reliability of the network. To do that, we use commonly known analytical measures, that is, MTTF and MTTD (*Mean Time to Disconnection*).

Mean time to failure represents the average amount of time before the system fails. It is calculated by providing a function that denotes the probability that the network is in an irreparable state. MTTD is the average time required to transition from the original state with no link failures to the disconnection state. This gives an idea of what requirements in terms of MTTR should a network operator demand from its service repair department in order to achieve a given MTTD.

The first parameter does not consider repairs of failed links and should be treated as a theoretical reference. Nevertheless, it is a good measure to objectively compare the topologies. In reality, broken links are repaired. Therefore, MTTD is more realistic and represents the mean time after which the connectivity in a network cannot be assured, given a certain value of MTTR.

3.1. Mean Time To Failure

For the reliability calculations, we use the state enumeration method, that is, we list all possible states and the sum of their probabilities. In case of MTTF, we model the behaviour of a system as a Markov chain, where states are related to different failure situations. We assume that failures as well as repair processes are memoryless, and we take into consideration failure/repair intensities in appropriate transitions. Therefore, we use homogeneous

Markov chains. The final step to obtain MTTF is the Laplace transform.

MTTF of a network with p-cycles can be obtained from the following formula:

$$MTTF = \int_0^\infty R(t)dt \tag{1}$$

where $R(t)$ is an all-terminal reliability function [24].

Equations (2) through (6) present the all-terminal reliability for p-cycles presented in Figure 2.

The (0:0) symbol describes the situation where there is no failure in a network. The (1:0) symbol indicates one failure in one of the p-cycles and none in the other. The remaining symbols are created in a similar way. Only the cases with all working links and those with failures that may be protected by p-cycles are considered in formulas 2, 3, 4, 5 and 6. In the formulas, k means the number of nodes, $2k$ represents the number of links and $r(t)$ is the reliability function of a single link.

$$R_a(t) = \underbrace{r^{2k}(t)}_{(0:0)} + \underbrace{2 \times \frac{k}{2} \times r^{\frac{k}{2}-1}(t) \times [1-r(t)] \times r^{\frac{k}{2}}(t) \times r^k(t)}_{(1:0)}$$
$$+ \underbrace{\left(\frac{k}{2} \times r^{\frac{k}{2}-1}(t) \times [1-r(t)]\right)^2 \times r^k(t)}_{(1:1)}$$
$$\tag{2}$$

$$R_b(t) = \sum_{i=0}^{\frac{k}{2}} \binom{\frac{k}{2}}{i} \times (4r^3(t) \times [1-r(t)])^i \times [r^4(t)]^{\frac{k}{2}-i} \tag{3}$$

$$R_c(t) = \underbrace{r^{2k}(t)}_{(0:0)} + 2 \times \left[\underbrace{r^{\frac{k}{2}+2}(t) \times \sum_{i=0}^{\frac{k}{2}-2} \binom{k}{i} r^{k-i}(t)(1-r(t))^i}_{(1:0)} + \underbrace{\left(\frac{k}{2}+2\right) r^{\frac{k}{2}+1}(t)(1-r(t)) \times \sum_{i=0}^{\frac{k}{2}-2} \binom{k}{i} r^{k-i}(t)(1-r(t))^i}_{(1:1)} \right] \tag{4}$$

$$R_d(t) = \underbrace{r^{2k}(t)}_{(0:0)} + \underbrace{2 \times k \times r^{k-1}(t) \times [1-r(t)] \times r^k(t)}_{(1:0)}$$
$$+ \underbrace{(k \times r^{k-1}(t) \times [1-r(t)])^2}_{(1:1)}$$
$$\tag{5}$$

$$R_e(t) = \underbrace{2 \times r^k(t) \times \sum_{i=0}^{k} \binom{k}{i} \times r^{k-i}(t) \times [1-r(t)]^i}_{n:0} + \underbrace{2 \times kr^{k-1}(t) \times [1-r(t)] \times \sum_{i=0}^{k} \binom{k}{i} r^{k-i}(t) \times [1-r(t)]^i}_{m:1} \tag{6}$$

that all links work without failures ($2k$ total links in the topology), (1:0) coefficient means that 1 link in a p-cycle is down and all other links work correctly ($r^{\frac{k}{2}}(t)$ reflects the number of links in a p-cycle without failure, $r^{\frac{k}{2}-1}(t)$ shows the number of links without failures in a p-cycle with one down link, $r^k(t)$ indicates the number of unprotected links, that is, placed outside the p-cycles), (1:1) coefficient means that 1 link in the first p-cycle is down, 1 link in the second p-cycle is down and all the other links work correctly [$r^{\frac{k}{2}-1}(t)$ reflects the number of links without failures in each p-cycle (here are two such p-cycles), $r^k(t)$ considers links placed outside the p-cycles].

In case (b), we make $k/2$ 4-link long p-cycles. In this scenario, all links are protected. The all-terminal reliability function can be constructed as in Equation (3). In this case, we have $k/2$ p-cycles. In each p-cycle up to 1 link may be down. In this equation, i means the number of p-cycles with 1 down link and $k/2 - i$ p-cycles without failures.

In case (c), there are two cycles, both traversing half of the network. The all-terminal reliability function can be constructed as in Equation (4). In each p-cycle, up to 1 on-cycle link and any number of straddling links may be down. (0:0) coefficient means that all on-cycle links work without failures ($k + 4$ links, which compose p-cycles), (1:0) coefficient means that 1 link in a p-cycle is down and all other on-cycle links work correctly ($r^{\frac{k}{2}+2}(t)$ reflects the number of links in a p-cycle with 1 failure, $r^{k-i}(t)(1-r(t))^i$ means a straddling link - up to $\frac{k}{2} - 2$ in each p-cycle), (1:1) coefficient means that 1 link in the first p-cycle is down, 1 link in the second p-cycle is down and any of straddling links may be down (($\frac{k}{2} + 2)r^{\frac{k}{2}+1}(t)(1 - r(t))$ reflects that one

on-cycle link in each p-cycle is failed, $r^{k-i}(t)(1 - r(t))^i$ means a straddling link -up to $\frac{k}{2} - 2$ in each p-cycle).

The all-terminal reliability function for case (d) can be constructed as in Equation (5). In this case, we have two p-cycles; in each p-cycle up to 1 link may be down. (0:0) coefficient means that all links work without failures ($2k$

In case (a), we create two p-cycles, one spanning over the inner ring and one spanning over the outer ring. The all-terminal reliability function can be constructed as in Equation (2). In the analysed case, we have two p-cycles: up to 1 link may be down in each. (0:0) coefficient means

links in topology), (1:0) coefficient means that 1 link in a p-cycle is down and all the other links work correctly ($r^{k-1}(t)$ reflects the number of links in the p-cycle with 1 failure and $r^k(t)$ considers the number of links in the p-cycle without failures), (1:1) coefficient means that 1 link in the first

	$MTTF(MTTF_\alpha)/MTTF_\alpha$				
k	case (a)	case (b)	case (c)	case (d)	case (e)
8	0.105	0.233	0.229	0.167	**0.469**
12	0.069	0.182	0.167	0.109	**0.305**
16	0.052	0.153	0.132	0.081	**0.226**
20	0.041	0.135	0.109	0.064	**0.180**
24	0.034	0.121	0.093	0.053	**0.149**
28	0.029	0.111	0.081	0.045	**0.127**
32	0.026	0.103	0.071	0.040	**0.111**
48	0.017	**0.082**	0.049	0.026	0.074
64	0.013	**0.070**	0.037	0.020	0.055

MTTF, Mean Time To Failure.

p-cycle is down, 1 link in the second *p*-cycle is down and all the other links work correctly ($r^{k-1}(t)$ considers the number of links in *p*-cycle with 1 failure).

The same layout as in case (d) is used in case (e), but here, both *p*-cycles cooperate. Similarly, all links are protected. The all-terminal reliability function can be constructed as in Equation (6). In this case, we have two *p*-cycles. In each *p*-cycle up to *k* links may be down; however, at that time, only up to 1 link may be down in the other *p*-cycle. (n:0) coefficient means that $n, (n \leqslant k)$ links are down in the first *p*-cycle and all links work properly in the second *p*-cycle ($r^{k-i}(t)$ reflects the number of working links in the *p*-cycle with failures, $r^k(t)$ shows the number of working links in the *p*-cycle without failures), (m:1) coefficient means that $m, (m \leqslant k)$ links are down in the first *p*-cycle and exactly 1 link is down in the second *p*-cycle ($r^{k-1}(t)$ reflects the number of working links in the *p*-cycle with one failure, $r^{k-i}(t)$ considers the number of working links in this *p*-cycle).

To obtain the exact values of MTTF of a network, the reliability function of a single link $r(t)$ needs to be known. However, as most of link failures are generated by cable cuts, and the ageing or other physical processes can be neglected, span failures are generally memoryless, thus characterised by a Poisson process with the rate λ.

Therefore, inter-failure times can be described by an exponential distribution with the average value $MTTF_\alpha = 1/\lambda$, where $MTTF_\alpha$ represents the MTTF of a single link. Although this value is related to the span length, to simplify the calculations, we consider equal link lengths, therefore equal $MTTF_\alpha$ values for each link.

The MTTF of the network considered in the paper, as a function of the number of nodes in the DRDA topology for the cases presented in Figure 2 (numbers written in bold show the best results) without repairs is obtained following Equations (7)–(11). The results that show the *MTTF* of the considered topology with *p*-cycles as a part of link $MTTF_\alpha$ are presented in Table I and illustrated in Figure 3.

$$MTTF_a(MTTF_\alpha) = \frac{13k^2 - 16k + 4}{8k(k-1)(2k-1)} \cdot MTTF_\alpha \quad (7)$$

$$MTTF_b(MTTF_\alpha) = \sum_{i=0}^{k/2} \frac{\binom{k/2}{i}4^i(-3)^{k/2-i}}{2k-i} \cdot MTTF_\alpha \quad (8)$$

$$MTTF_c(MTTF_\alpha) = \frac{5k^2 + 30k + 44}{2(k+2)(k+3)(k+4)} \cdot MTTF_\alpha \quad (9)$$

$$MTTF_d(MTTF_\alpha) = \frac{5k^2 - 5k + 1}{2k(k-1)(2k-1)} \cdot MTTF_\alpha \quad (10)$$

$$MTTF_e(MTTF_\alpha) = \frac{7k(k-1) + 2}{k(k-1)(2k-1)} \cdot MTTF_\alpha \quad (11)$$

As we can see, the worst results are observed for case (a). In this configuration, the 'dual attachment' links (joining the inner and outer rings) are not protected. Therefore, each failure cannot be repaired, and the connectivity cannot be assured. This situation was partially and fully eliminated in cases (c) and (d), respectively, where *p*-cycles protect more/all links in the DRDA network. Because of that, the MTTF is greater in those cases compared to case (a).

The case (b) shows that many smaller *p*-cycles work better than in cases (a), (c) and (d). This observation is consistent with our presumptions. If we have more *p*-cycles,
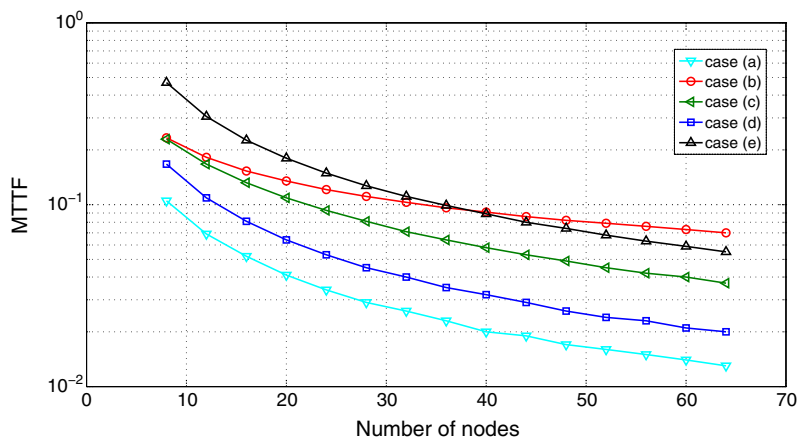

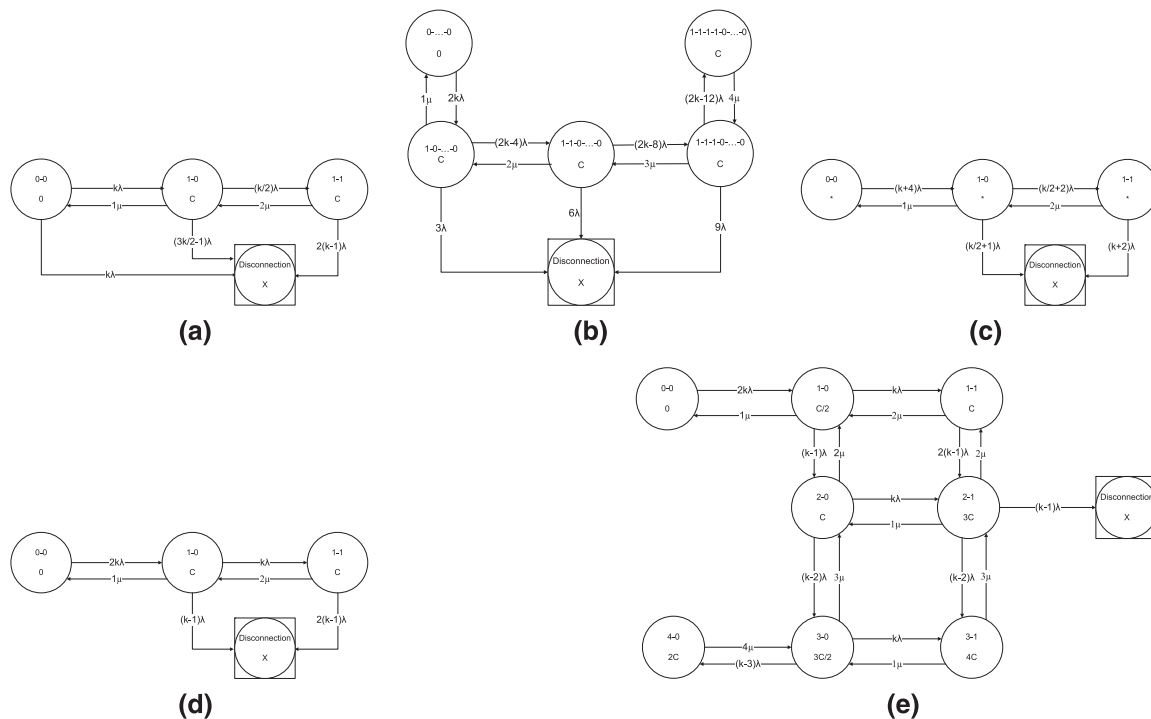**Figure 3.** Mean Time To Failure values for *p*-cycles from Figure 2.

Figure 4. Continuous-Time Markov Chains for several *p*-cycle configurations.

the number of links that may fail at the same time without loosing connectivity in a network is greater. As a result, the MTTF for such configurations is usually better. On the other hand, the best results are observed for case (e), with two interacting *p*-cycles proposed, if the number of nodes in the network is lower or equal to 32. The size of a DRDA network composed of 32 nodes may be very large (it depends on span lengths). In this case, the best MTTF values are observed because the *p*-cycles cover all nodes in the network and they protect links in a coordinated way (each link is protected by both *p*-cycles).

Based on the results, we can conclude that for small DRDA networks (up to 32 nodes), the *p*-cycle configuration shown in Figure 2(e) is the best solution. However, for larger networks, providing many 4-link long *p*-cycles gives better results in terms of MTTF. It is more probable that in larger networks (composed of numerous number of nodes) with only one or two *p*-cycles covering all nodes, two or more failures occur at the same time in the *p*-cycle. If we have more *p*-cycles in the same network, the probability of disconnection is lower. This observation is characteristic to *p*-cycles in general, as they are not supposed to span over numerous hops [25].

3.2. Mean Time To Disconnection

As noted in [22], the following analysis assumes that links in the DRDA happen to fail independently. Now, links are assumed to be repaired by the network operator following again the exponential distribution with rate μ. Now,

μ^{-1} is referred to as the MTTR. The target is to find the *Time To Disconnection* probability distribution function of a generic *k*-DRDA topology and derive its MTTD average value. We assume that an observed average link failure value of Mean Time Between Failures (MTBF) is given and that the network operator can guarantee a certain average link repair time given by its MTTR value.

To simplify the model, no more than four link failures are assumed to occur simultaneously, which is highly improbable (actually less than 10^{-6} for $MTBF = 60$ days and traditional MTTR values of hours and days [22]).

With these assumptions, a given *k*-node DRDA can be easily characterised and analysed with respect to its reliability by *Continuous-Time Markov Chain* (CTMC) [26]. Figure 4 shows the CTMC for the different *p*-cycle configurations proposed in Section 2, which can be read as follows. The generic state $(n_1 : \ldots : n_i : \ldots : n_{f(k)})$ gives the number of failures on the different *p*-cycles, together with the required units of backup capacity C_b for that state. For instance, the state labelled (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 Figure 4 also gives the transition probabilities between states. For instance, transition from state (0:0) to state (1:0) occurs with rate $2k\lambda$, because 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)
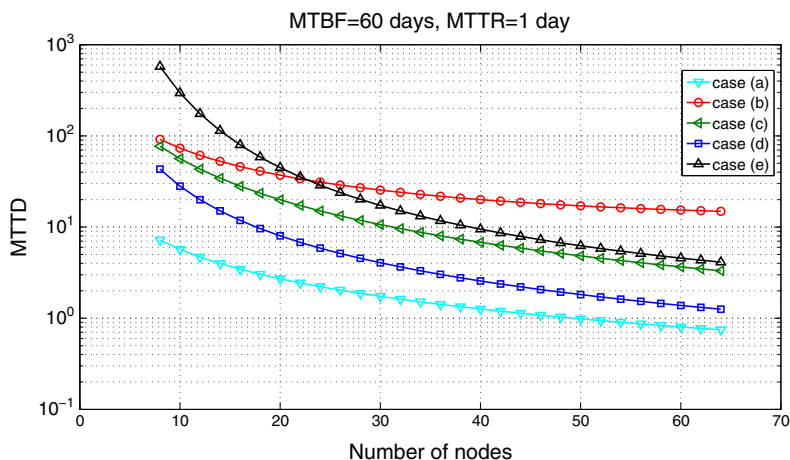
Figure 5. Mean Time To Disconnection for several *p*-cycles configurations.

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 failure on the dual *p*-cycle is recovered. The same reasoning applies to the rest of state transition rates. Finally, the state *Disconnection* 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 $(0 : \ldots : 0)$, it is just required to choose the entry $((0 : \ldots : 0), Disconnection)$ 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.

Figure 5 shows the MTTD values for different k-size DRDAs (varying from $k = 8$ nodes to $k = 64$ nodes), for $MTBF = 60$ days and $MTTR = 1$ day. It is worth noting that k must be a multiple of 4 in order to define the two dual *p*-cycles. First of all, there is a decreasing trend of MTTD with respect to k, as when there are more links in the network, the probability of failure grows significantly. Moreover, in case (e), the transition probability to the disconnection state depends on the number of nodes, whereas, in case (b), this probability is constant (Figure 4). This shows that *p*-cycle configuration as proposed in case (e) is suitable only for smaller networks. For instance, an 8-node DRDA, using a collaborative *p*-cycle, shows $MTTD = 577$ days, whereas a 32-node DRDA gives a much smaller $MTTD = 15$ days.

Concerning different configurations, it can be observed that the obtained results are similar to those presented in the previous section. That is, the worst case is (a), where two *p*-cycles without cooperation are considered. If the number of nodes in the topology is small (less than 24), the most resilient solution (in terms of MTTD) is case (e),

where two dual collaborative *p*-cycles are defined. However, for larger topologies (if the number of nodes is greater than 24), providing many 4-link long *p*-cycles, that is, case (b), gives better results in terms of MTTD.

In order to assess how MTTR influences MTTD, Figure 6 shows the MTTD for different values of MTTR and numbers of nodes, for the two most resilient solutions obtained in the previous analysis, namely, case (e) and case (b). It can be observed that case (e) is better than case (b) for every value of MTTF (in the typical range of 0–5 days) when $k = 8$ nodes, whereas if $k = 16$ nodes, both cases are similar when MTTF is greater than 2 days. Finally, when $k = 32$, case (b) is better than case (e) if only MTTF is higher than 12 h.

3.3. Required backup capacity

The *p*-cycles presented in this paper ensure that a number of link failures may be repaired and the connectivity between all the nodes is still secured. However, we need to ensure additional capacity on the selected links to serve the redirected traffic. In this section, we present the analysis of required backup capacity in single links and in the whole network.

*n means all straddling links that may fail, n_1 means straddling links in one *p*-cycle that may fail and n_2 means straddling links in second *p*-cycle that may fail

The results of our analysis are presented in Table II. C_b per link means how much capacity per link in each *p*-cycle needs to be added to serve the additional traffic if failures occur. On the other hand, the C_b per network shows how much additional capacity we need to buy in the whole network to serve the backup traffic. For cases (a), (b) and (d), we need the additional C per each link in each *p*-cycle, which repairs a failure. Thus, there is a need for C multiplied by the number of on-cycle links additional capacity in the network. In cases (c) and (e), it is more complex to estimate the demand on capacity, which demands on the number of links we want to protect (in case (c), we may
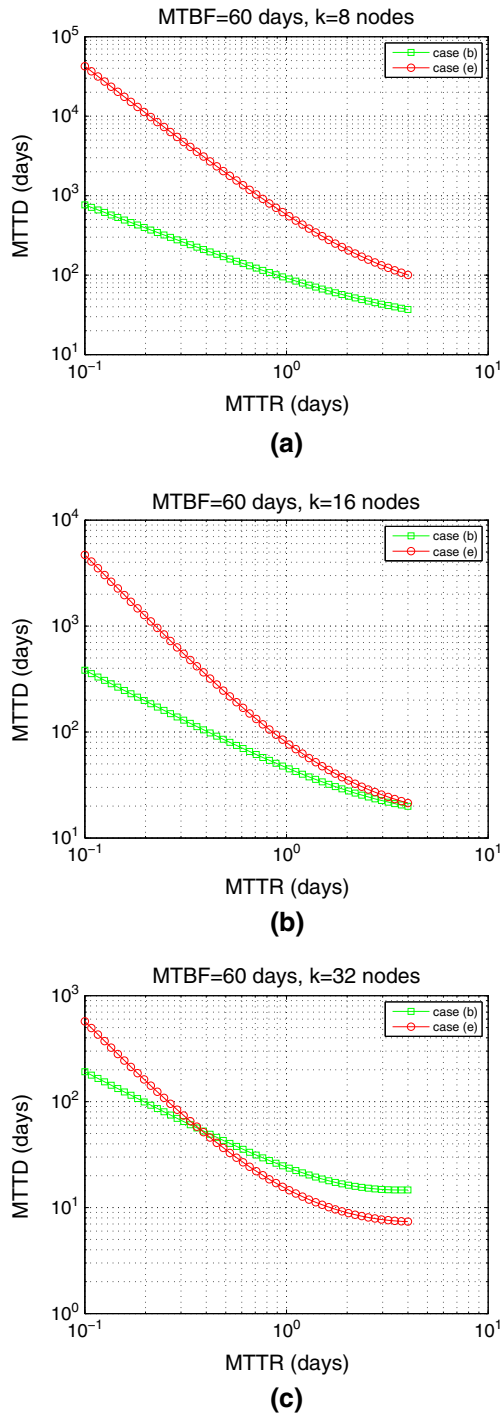
Figure 6. Mean Time To Disconnection for different combinations of Mean Time to Repair and number of nodes.

protect up to one failed on-site link and all straddling links, whereas in case (e), we may protect up to one failure in a *p*-cycle and all links in the second *p*-cycle).

The recovery column shows how the corresponding failure is repaired. O-C means the on-cycle repair strategy,

which is used when a failure occurs in one of the links belonging to a *p*-cycle; it is repaired by the alternative route on the cycle. F-S denotes full-straddling repair strategy, which is used when a protected off-cycle link fails; it is repaired by the *p*-cycle and the traffic is balanced over two alternative routes. S-S is the semi-straddling repair strategy, which is used when a straddling link fails but the *p*-cycle is not fully functional either; in this case, the redirected traffic from the failed straddling link cannot be sent over two paths, as only one is available. All the mentioned strategies have been described in details in [22].

The results in Table II show that, when there is only one failure of on-cycle links in a network, the best results are observed for case (a) (where not all links are protected) and for case (e). In case of two failures (1:1), the configuration (a) is the best. More failures can be repaired only when case (b), (c) or (e) is implemented; however, in case (c), up to one on-cycle link in each *p*-cycle may fail. With the same additional capacity as in case (e), in case (b), we may protect more links. This case is also more suitable for bigger networks along with lower needs for additional capacity. The analysis shows that taking into consideration only the need for additional capacity, the (e) configuration may be worse than the other proposals under specific conditions (when not all links are protected or when *p*-cycles are small and have up to one failure). On top of that, the values of the MTTF and MTTD presented in previous sections are significantly greater in case (e) than for the other cases in relatively small networks. Network operators may decide by themselves, which of the analysed *p*-cycle configurations is the most suitable for them.

In case (e), we are also able to provide protection when more links fail at the same time; yet, this cases require much more additional capacity. However, we need to note that the sole connectivity between all nodes in the network is assured even when all links in one *p*-cycle fail. If we do not have enough capacity to serve all redirected traffic, the transmission will be slowed down but not disconnected. Such an advantage is not observed for the other proposals.

If we look at the example for $k = 8$ and assume the maximum of two simultaneous link failures in the network, we can see that for cases (b), (d) and (e), which are the most capacity consuming examples, we need to increase each link capacity twice (in case (c), we may need even more capacity when we decide to protect also straddling links). In comparison to other architectures, for example, RPR, this feature of DRDA is very good. In RPR, we also need to multiply each link capacity by two in case of a link failure. However, in RPR, we can repair two failures only if they occur between two corresponding nodes. The strong advantage of case (e) is that any two failures will be repaired, whereas topologies (b) and (d) do not present that feature.

Table II. Capacity requirement comparison.

Topology	Failure	Recovery strategy	C_b per link	C_b per network
(a)	(1:0) or (1:1)	O-C	C	kC
(b)	up to 1 link in each p-cycle	O-C	C	$2kC$
	(0 : 0)	n F-S	$nC/2, n \in < 0, k-4 >$	$(k+4)nC/2$
(c)*	(1 : 0)	n_1 S-S +1 O-C	$C + n_1 C$	$(C + n_1 C)(k/2 + 2)$
		n_2 F-S	$n_2 C/2$	$(n_2 C/2)(k/2 + 2)$
	(1 : 1)	n_1 S-S +1 O-C	$C + n_1 C$	$(C + n_1 C)(k/2 + 2)$
		n_2 S-S +1 O-C	$C + n_2 C$	$(C + n_2 C)(k/2 + 2)$
(d)	(1:0) or (1:1)	O-C	C	$2kC$
	$(n : 0)$ with $1 \leq n \leq k$	n F-S	$nC/2$	knC
(e)	(1 : 1)	2 S-S	C	$2kC$
	$(m : 1)$ with $2 \leq m \leq k$	m S-S + 1 O-C	$(m+1)C$	$2k(m+1)C$

4. CONCLUSION

The DRDA architecture is a new proposal for the high-speed reliable transmission of data in the metropolitan area. In such a network topology, the protection possibilities provided by implementing several link-disjoint p-cycles are quite large. It is possible to protect each link in a topology or only a part of them. It depends on the chosen p-cycle configuration. Of course, the more links we protect, the more reliable network is. The results presented in this paper confirm this statement.

This work provides a reliability analysis for the most sensible p-cycle configurations in the considered DRDA topology. In order to assess the reliability of DRDA, MTTF and MTTD indicators were used. As shown, when the number of nodes is small, two dual p-cycles with cooperation provide the best solution in terms of both MTTF and MTTD. However, for large topologies (more than 24 nodes), it is generally a better solution to split the protection rings into several small 4-link p-cycles.

The DRDAs with 24 nodes may also be quite large. Our observations indicate that ring-based networks with 12 (which corresponds to 24 nodes in DRDAs) or larger number of nodes are rarely used. The studies presented in this paper confirm that, in most cases, two interworking p-cycles should be used to protect links in the DRDA networks. It is worth to note that in this case, we protect more links in comparison to the other solutions. Moreover, even if we do not have enough capacity to serve all redirected traffic, we still ensure connectivity between all nodes. In such a case, traffic is sent only with a lower rate. Finally, the network administrators are free to choose how much additional capacity they want to inject in their networks. More spare capacity generates costs but improves reliability.

This information is of special interest for network operators when they have to deploy a protection mechanism in their MAN, which demand full-time any-to-any connectivity, such as the networks that distribute Internet Protocol television (IPTV) services.

ACKNOWLEDGEMENT

REFERENCES

1. Yao S, Yoo S, Mukherjee B, Dixit S. All-optical packet switching for metropolitan area networks. *IEEE Communications Magazine* 2001; **3**(39).
2. Resilient packet ring (RPR) access method and physical layer specifications. *802.17 IEEE Standard*, June 2004.
3. Grover W, Stamatelakis D. Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration. In *IEEE ICC 1998*: Sydney, Australia, IEEE, 1998; 537-543.
4. Wu B, Yeung K, Xu S. ILP formulation for p-cycle construction based on flow conservation. In *IEEE Globecom 2007*: Washington DC, USA, IEEE, 2007; 2310-2314.
5. Wu B, Yeung K, Ho PH. ILP formulations for p-cycle design without candidate cycle enumeration. *IEEE/ACM Transactions on Networking* 2010; **18**(1): 284–295.
6. Grover W, Kodian A. Failure-independent path protection with p-cycles: efficient, fast and simple protection for transparent optical networks. In *ICTON 2005*: Barcelona, Spain, IEEE, 2005; 363–369.
7. Kamal A. 1+n network protection for mesh networks: network coding-based protection using p-cycles. *IEEE/ACM Transactions on Networking* 2010; **18**(1): 67–80.
8. Menth M, Martin R, Hartmann M, Spörlein U. Efficiency of routing and resilience mechanisms in packet-switched communication networks. *European Transactions on Telecommunications* 2010; **21**(2): 108–120.
9. Cao C, Rouskas GN, Wang J, Tang X. Hybrid FRR/p-cycle design for link and node protection in MPLS networks. *AEU - International Journal of Electronics and Communications* 2013; **67**(6): 470–478.
10. Szigeti J, Gyarmati L, Cinkler T. Multidomain shared protection with limited information via MPP and p-cycles. *Journal of Optical Networking* 2008; **7**(5): 400–409.

11. Gyarmati L, Cinkler T, Trinh TA. Path-based multipath protection: resilience using multiple paths. *Transactions on Emerging Telecommunications Technologies* 2012; **23**(7): 660–671.

12. Guo L, Cao J, Wang X, Wei X, Gai Q, Ning Z, Yu C. Survivable routing algorithm with mixed shared protection in fault-tolerant GMPLS multi-layered optical networks. *European Transactions on Telecommunications* 2010; **21** (4): 312–323.

13. Choi H, Subramaniam S, Choi HA. Loopback recovery from double-link failures in optical mesh networks. *IEEE/ACM Transactions on Networking* 2004; **12**: 1119–1130.

14. He W, Sridharan M, Somani AK. Capacity optimization for surviving double-link failures in mesh-restorable optical networks. *Photonic Network Communications* 2005; **9**: 99–111.

15. Feng T, Long L, Kamal AE, Ruan L. Two-link failure protection in WDM mesh networks with p-cycles. *Computers Networks* 2010; **54**: 3068–3080.

16. Wu J, Liu Y, Yu C, Wang X, Zhao J. Multicast protection based on enhanced intelligent p-cycle method in optical mesh networks. *Optical Engineering* 2013; **52** (1): 015 008–015 008.

17. Kodian A, Grover W. Multiple-quality of protection classes including dual-failure survivable services in p-cycle networks. In *BroadNets 2005*: Boston MA, USA, IEEE, 2005; 231–240.

18. Wang H, Mouftah H. P-cycles in multi-failure network survivability. In *ICTON 2005*: Barcelona, Spain, IEEE, 2005; 381–384.

19. Zhang F, Zhong WD, Jin Y. Optimizations of p-cycle-based protection of optical multicast sessions. *Journal of Lightwave Technology* 2008; **26** (19): 3298–3306.

20. Onguetou DP, Grover WD. Approaches to p-cycle network design with controlled optical path lengths in the restored network state. *Journal of Optical Networking* 2008; **7**(7): 673–691.

21. Cholda P, Jajszczyk A. Reliability assessment of p-cycles. In *IEEE Globecom 2005*: St. Louis, USA, IEEE, 2005; 5.

22. Santiago del Rio PM, Hernandez JA, Aracil J. *et al.* A reliability analysis of double-ring topologies with dual attachment using p-cycles for optical metro networks. *Computer Networks* 2010; **54**: 1328–1341.

23. http://projects.celtic-initiative.org/tiger2/.

24. Shooman ML. *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. John Wiley and Sons, Inc.: New York, NY, 2002.

25. Cholda P, Jajszczyk A. Reliability assessment of optical p-cycles. *IEEE/ACM Transactions on Networking* 2007; **15**(6): 1579–1592.

26. Ibe OC. *Markov Processes for Stochastic Modeling*. Elsevier Science & Technology Books: University Press, Cambridge, 2009.