Formal Specification and Dependability Analysis of Optical Communication Networks

Umair Siddique*, Khaza Anuarul Hoque†, Taylor T. Johnson‡
*Dept. of Computing and Software, McMaster University, Canada
†Dept. of Computer Science, University of Oxford, UK
‡Dept. of Electrical Engineering & Computer Science, Vanderbilt University, USA

***Abstract*—Network dependability reflects the ability to deliver continuous services even after failures, such as man-made or natural disturbances, e.g., storms, hurricanes, and floods, etc. In the last decade, optical networks have been increasingly deployed to provide multicast traffic in metropolitan areas. In this paper, we provide a formal specification of double-rings with dual attachments (DRDA) topologies of optical networks using Continuous-Time Markov Chains. Our formal modeling includes the concept of pre-configured protection cycles (p-cycles), which provide effective fault tolerance against link-failures in optical networks. Our approach is generic enough to handle networks of any size that are prone to any combinations of link failures. We formally specify several dependability properties using Continuous Stochastic Logic (CSL). We then provide a quantitative evaluation of these properties using the PRISM model checker. We observe that such formal analysis can provide critical information at early design stages to network operators for designing highly-dependable optical networks in metropolitan areas (e.g., availability on the order of 99.99% or 99.999%).**

I. Introduction

The ever increasing growth of services over the Internet has been resulted in a demand for huge bandwidth in communication networks. However, traditional electronic communication has already reached a point where this issue cannot be addressed anymore. On the other hand, optical technology has the potential to meet the future speed and bandwidth requirements. Future communication systems will be based on electronic-photonic convergence as mentioned in MIT's first Communications Technology Roadmap (CTR) [1]. Practical demonstrations have shown the ability of optical networks to achieve the line-rate capacities up to Tera-bits/second using wavelength division multiplexing (WDM) techniques [2]. These features in optical networks do not eliminate the need for designing survivable network architectures that have the ability to maintain an acceptable level of service during and after failures. Moreover, the failure tolerance of optical metropolitan area networks has become more important due to their direct impact on cost and safety-critical application domain.

In practice, optical fiber cuts are considered to be the most common failures in optical networks, which result in a large number of link failures impacting many stack holders including government offices, banks and hospitals. There are estimates that long-haul networks annually suffer 3 cuts for every 1000 miles of optical fiber [3]. For a large network of $50,000$ miles of optical fiber cable, that would be around 150 cuts per year. Node failures is another possibility in optical networks which are less frequent than link-failures. Catastrophic events (e.g., fires, floods, and earthquakes, etc.) are rare, but can cause a widespread disruption of network services. For example, the fire at the Toronto central office of Bell Canada in 1999 and flooding and power outages at central offices due to Hurricane Katrina in 2005 [4], impacted numerous information and communication technology (ICT) services. Considering the above mentioned factors, it is indispensable to design a dependable network that can protect communication services against optical link-failures and possesses the ability to provide service beyond the failure of their components. Indeed, several survivability mechanisms have been designed to protect against single link or single event failures in optical networks. However, multiple failure restorability is becoming more important as it provides more realistic model of real-world networks [5]. One of the most popular protection schemes is preconfigured protection cycles (also named p-cycles) [6]. The p-cycles based protection shares the advantages of resilient packet rings mechanisms (i.e., fast recovery time) and meshed-protection techniques (i.e., high capacity efficiency). In the last decade, p-cycles have been used to design real-world networks and which have also been the subject of analysis.

Formal methods provide a rigorous framework to verify specifications of real-world software and hardware systems during different phases of their design life-cycle. Recently, formal methods (in particular theorem proving) have been applied to verify critical properties of optical systems (e.g., [7], [8]). However, these applications are limited only to physical components of optical systems, which prevents their usage to analyze interesting dependability metrics (e.g., availability and maintainability) in optical networks. On the other hand, *probabilistic model checking* [9] provides the basis to formally specify and verify such dependability properties of real-world systems. The construction of a system model (usually a Markov chain or a Markov process) and the verification of properties in probabilistic model checking are based on exhaustive state-based exploration techniques. The property satisfaction through model checking ascertain that the property holds for all possible behaviors of a given system. This is in contrast to simulation and testing based approaches, where results are mostly based on certain scenarios and sampling periods. Moreover, these advantages of model checking make it an attractive verification method as compared to traditional discrete-event simulations, in which approximate results are computed using averaging from a large number of random samples. The use of formal methods is even recommended by international organizations (e.g., Federal Avionics Association (FAA)) and certification standards (e,g., DO-178C). Some successful applications of probabilistic model checking include aerospace systems [10] and communication protocols [11].

978-3-9815370-8-6/17/$31.00

In this paper, we apply probabilistic model checking to conduct the dependability analysis of networks based on the p-cycle protection mechanism. The main contributions of the paper are as follows:

- we build a Continuous-Time Markov Chain (CTMC) model of emerging Double-Ring topologies with Dual Attachment (DRDA) [12] which consist of two dual p-cycles. The proposed (CTMC) model represents a generic k node network with the possibility of any number of link failures.
- we formally specify the DRDA model and associated link-failure strategies in PRISM model checker. In fact, we build modules to represent link-failures and use the notion of rewards to quantify some important network metrics such as unavailability, repairability and total time spent in a state.
- we formalize the dependability metrics (e.g., *disconnection probability*, *expected time to disconnection*, *expected number of repairs*, etc.) of DRDA based optical network in Continuous Stochastic Logic (CSL). We provide quantitative evaluation of these properties using the PRISM model checker.

To the best of our knowledge, p-cycles based network dependability analysis has not been previously performed with any formal methods techniques. We believe that our proposed work can provide an accurate and early assessment of network dependability while saving the overall design effort, cost and time. Moreover, our work can be considered a step towards the goal of model checking assisted optical network designs on the similar lines of the recent work [13] related to wireless networks.

The rest of the paper is organized as follows: Section II outlines the preliminaries of p-cycles and DRDAs along with a brief introduction of PRISM model checker. The details of multiple link-failures, associated recovery strategies and CTMC modeling are presented in Section III. We describe the results of the formal analysis of dependability properties in Section IV. Finally, Section V concludes the paper and highlights some future research directions.

II. Background

In this section, we review p-cycles, DRDA and provide a brief account of PRISM model checker.

A. Basics of p-Cycles

The preconfigured protection cycle or p-cycle (originally introduced in [6]) consists of a set of links connected in a circular architecture as shown in Figure 1 (a), where v_i represents nodes. Each link in a p-cycle, has a spare capacity of c units which help in transmitting data in case of a link failure in the network. The distinguishing feature of p-cycle over ring based architecture is its ability to configure the spare capacity into pre-connected cycles which provides extremely fast restoration. A p-cycle in a network can provide a protection against two types of failures:

On-cycle Span Failure: In this type, a failure occurs on a link that belongs to the p-cycle. This type of failure can be recovered by switching the traffic on the opposite direction of the p-cycle (as shown in Figure 1 (b), where the dashed lines represent an alternative path through nodes v_i).

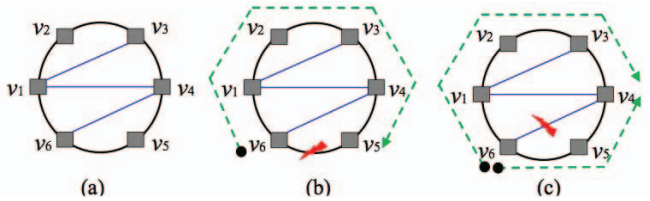

Fig. 1. Schematic representation of p-cycle

Straddling Span Failure: In this type, a failure may happen on a link which does not belong to the p-cycle. The failure in this case can be recovered through the links on p-cycle since the edges of the failed link are connected to two nodes of the p-cycle (as shown in Figure 1 (c)). Note that a p-cycle provides a protection to not only its member links but also the links which are connected to its nodes, which provide the redundancy required for network protection.

B. Double-Ring Topology with Dual Attachment

A Double-Ring topology with Dual Attachment (DRDA) consists of two duplex (bi-directional) rings of the same number of links. The two rings are referred to as *inner* and *outer* ring and their corresponding nodes are connected to each other through a duplex link as shown in Figure 2 (a). The size and characteristics of a given DRDA is determined by the total number of nodes. A DRDA with k nodes is called k-DRDA and it contains $2k$ links which can fail, e.g., Figure 2 (a), shows an 8-DRDA which consists of 16 links. In order to form two p-cycles on a given DRDA, the number of nodes k should be even as shown in Figure 2 (b). Note that two p-cycles on DRDA covers all the nodes in the k-DRDA topology which result in the connection among any two nodes of DRDA. Moreover, the associated links of the two p-cycles are disjoint which provide an effective protection mechanism in case of a failure in the network. These two features of DRDA architecture provide the capability to handle both on-cycle span failure and straddling span failure on the actual p-cycle (Figure 2 (b) left) or its dual counterpart (Figure 2 (b) right).

C. PRISM Model Checking Tool

PRISM [14] is a well known tool for the formal modeling and verification of stochastic systems. The current version of the tool supports four types of probabilistic models: Discrete-time Markov Chains (DTMCs), CTMCs, Discrete-time Markov Decision Processes (MDPs), and Probabilistic Timed Automata (PTA). A PRISM model is defined as the composition of one or more elementary systems known as `modules`. Formally analyzing a system is done with respect to one or more properties. The property specification language in PRISM is mainly based on temporal logic, which offers an unambiguous means of describing a broad range of properties. The specification language for properties of the probabilistic models to be analysed in PRISM is based on temporal logic, in particular PCTL [15] and CSL (CSL is an extension of PCTL

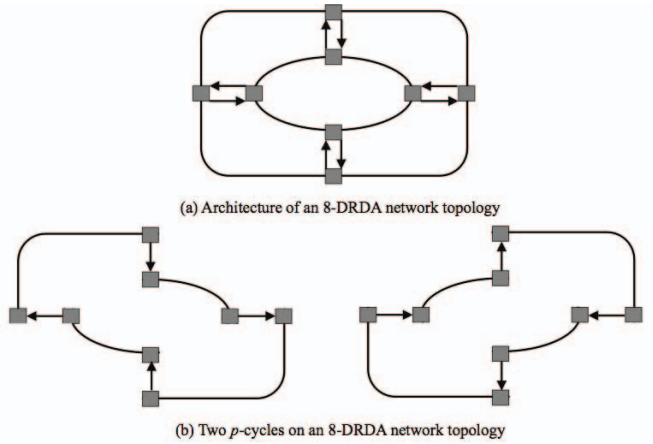

Fig. 2. Architecture of DRDA

for CTMCs) [16]. The principal operators are P, S and R which refer, respectively, to the probability of an event occurring, the long-run probability of some condition being satisfied, and the expected value of the models costs or rewards. Rewards can be used to specify a wide range of measures of interest, for example, the number of correctly delivered packets or the time that the system is operational.

III. Formal Modeling of Optical Network

In this section, we describe the formal modeling of optical networks in metropolitan areas assuming two main conditions: a) the network should consist of two duplex rings with equal numbers of nodes (indeed this number should be even to form the two p-cycles with mutually disjoint links); b) all nodes of the inner ring should be connected to corresponding nodes of the outer ring with two connections allowing two-way communication.

A. Strategies to Recover Single Link Failure

Generally, a span failure on one of the two dual p-cycles in k-DRDA can be recovered by three possible ways:

Strategy 1 (*Full-Straddling Span Failure (F-S)*)**:** In this case, a span failure on one p-cycle can be recovered by the dual p-cycle using two distinct paths.

Strategy 2 (*Semi-Straddling Span Failure (S-S)*)**:** In this case, a span failure on one p-cycle can be recovered by the dual p-cycle using only one shortest available path.

Strategy 3 (*On-cycle span failure (O-C)*)**:** In this final case, a span failure is recovered by its actual p-cycle by reversing the direction of the communication.

B. Recovery Mechanism for Multiple Link Failure

In practical situations, a network may suffer from multiple link failures due to factors like accidental cuts of fiber cables. We can compose the above mentioned three strategies to deal with such situations depending upon the pattern of failures on each p-cycles in a given DRDA topology. Formally, we denote the state of a k-DRDA by a pair (m:n), where m and n represent number of link failures on the two p-cycles at a given instant of time. Note that $0 \leq$m$\leq k$ and $0 \leq$n$\leq k$, as each p-cycle of the k-DRDA contains k links.

We summarize four possible cases of multiple link failures and corresponding recovery strategies in TABLE I.

Note that any combination of multiple failures (except case 4) can be recovered using the composition of one of the three recovery strategies, i.e., F-S, S-S and O-C.

TABLE I. Multiple Link Failures and Recovery Strategy

Cases	Failure State	Recovery Strategy
Case 1	(m:0) where ($1 \leq m \leq k$)	m F-S
Case 2	(1:1)	2 S-S
Case 3	(m:1) where ($2 \leq m \leq k$)	m S-S and 1 O-C
Case 4	(m:n) where ($2 \leq m, 2 \leq n$)	Not applicable

C. Continuous-Time Markov Chain Modeling for DRDA

It is reasonable to consider that failures happen independently among optical links in a given k-DRDA. Furthermore, the assumption of memoryless behaviour of failures can be taken if the time between failures is exponentially distributed (with a rate λ). Along the same lines, we can assume that links are repaired by the network operator following an exponential distribution with a rate μ of repaired links per unit of time. The parameters λ^{-1} and μ^{-1} are referred to as Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR), respectively. The above mentioned aspects allow us to build a generic Continuous-Time Markov Chain model for a given k-DRDA topology, as shown in Figure 3. The states in the Markov model are represented by (m:n) which provides the number of failures on the two p-cycles of the DRDA. In our model, we consider that the outer p-cycle provides the protection to the inner p-cycle that means the number of failures n cannot be greater than m.

The initial state of the CTMC (Figure 3) is given by (0:0), i.e., no link failure on p-cycles. In case of first link failure, the state of the model changes to (1:0), with a transition rate of $2k\lambda$, as any of the $2k$ links of k-DRDA can fail in initial state. The link failure in this state can be fixed by a repair rate μ by a network operator. Similarly, a link failure on the second p-cycle leads to the transition from state (1:0) to (1:1). The recovery from this state can be done at a rate 2μ due to the application of semi-straddling strategy as listed in TABLE I. In Figure 3, the dotted arcs and corresponding labels indicate the multiple transitions between tail and head states, and transition rates, respectively. The ranges of the intermediate states are listed as model parameters (e.g., x, p, q, etc.) in Figure 3. We summarize in TABLE II the generic cases of link failure and recovery along with the transition rates. For example, the repair rate for the link failure on the second p-cycle (represented by n, last case in TABLE II) result in two subcases: a) if the current state represent equal number of failures on both p-cycles then we require the application of the semi-straddling strategy m and n times, respectively; b) more failures on first p-cycle require the application of n time on-cycle strategy to recover the fault on the second p-cycle. The rates for the failure and recovery transitions for intermediate states which follow cases 1 and 4 of TABLE II are represented by the functions R and Z as shown in Figure 3.

We formalize the specification of p-cycles along with their associated failures and repairs in PRISM modeling language.

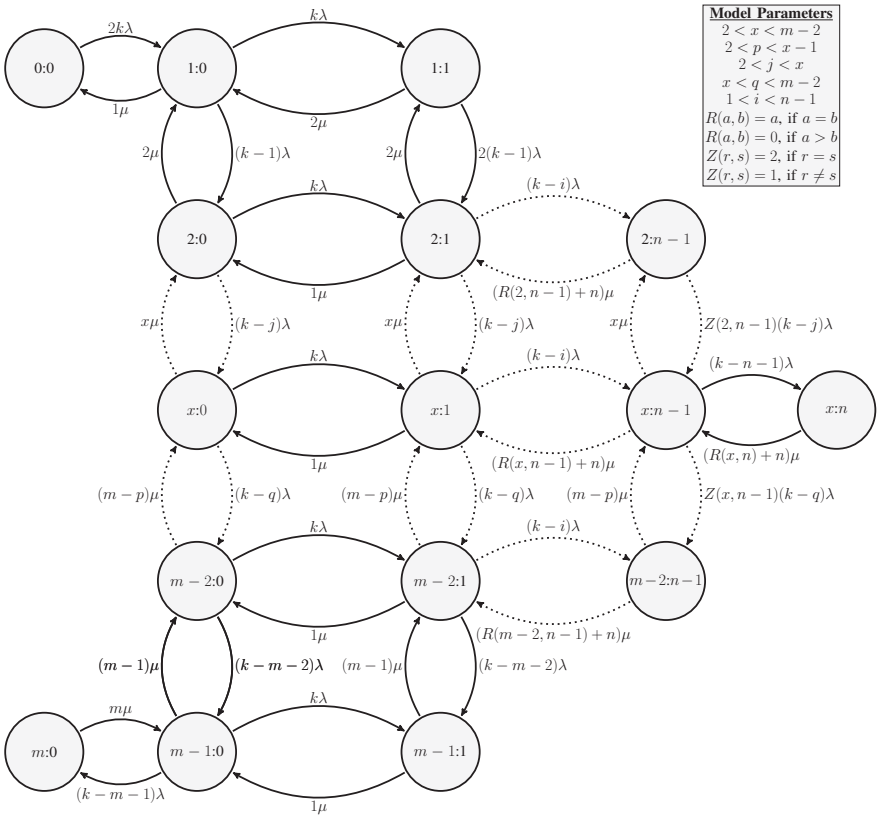

Fig. 3. CTMC model for a k-DRDA network topology

TABLE II. CASES OF LINK FAILURE AND RECOVERY ON TWO p-CYCLES

No.	Failure or Repair on Rings	Transition Rates
1	Failure on m	$2(k-m)\lambda, m = n$ $(k-m)\lambda, m \neq n$
2	Failure on n	$(k-n)\lambda$
3	Repair on m	$m\mu$
4	Repair on n	$(m+n)\mu, m = n$ $n\mu, m > n$

We build two modules namely `PCycle_M` and `PCycle_N`, which represents the current value of *m* and *n* in a generic state *(m:n)*. We also use three `reward` structures in our model: a) the `reward` structure `unavailable` assigns reward of 1 to the states satisfying the `formula` *disconnect*; b) the `reward` structure `repair` assigns a reward of 1 to all the repair transitions in the model with the actions labels that are specified inside the structure; and c) the `reward` structure `total_time` is used to compute the total elapsed time.

As mentioned above, the CTMC model discussed in this section is generic and can be applied to DRDA network topology of any size (k). In the next section, we provide the quantitative analysis to demonstrate that such a model of metro networks can be used to get an early dependability assessment.

IV. QUANTITATIVE ANALYSIS

In order to demonstrate the effectiveness of proposed model, we evaluate various properties of interest to analyze a

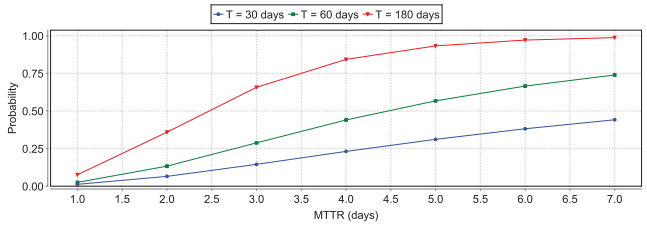

Fig. 4. Disconnection probability for different MTTRs given MTBF

10-DRDA for different values of MTBFs, MTTRs and mission times. The maximum number of multiple link failures are assumed to be 6. Note that, since the model is parametric, a CTMC model reflecting different number of link failures can be obtained automatically by re-initializing the PRISM model without any extra effort. The relationship between the size of the CTMC model and the number of multiple link failures is shown in TABLE III. We used PRISM v4.1 for all the analysis presented in this section.

TABLE III. CTMC MODEL SIZE FOR DIFFERENT NUMBER OF MULTIPLE LINK FAILURES

No. of Link Failures	No. of States	No. of Transitions
6	16	42
8	25	72
10	36	110
15	72	240
20	121	420

In practical situations, it is important to analyze and find

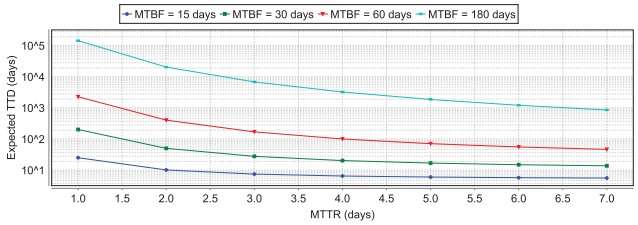

Fig. 5. Expected Time To Disconnection (TDD) for different combinations of MTTR and MTBF

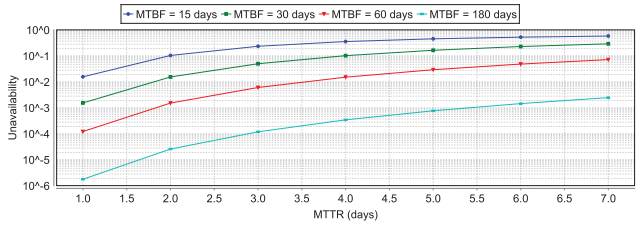

Fig. 6. Expected unavailability for different combinations of MTTR and MTBF

the appropriate MTTR that a network operator must ensure that will guarantee a given disconnection probability for given period of mission time. This query can be formalized in PRISM using CSL as following:

Property 1: `P=? [ F[0,T] (disconnect)]` - "*the probability that the network gets disconnected within 0 to T days.* "

We evaluate property 1, i.e.,the disconnection probability for a mission time of one month (30 days), two months (60 days) and one half year (180 days) given different values of MTTR and MTBF = 60 days. The obtained results are shown in Figure 4. This figure shows that with the increasing MTTR values, the disconnection probabilities also increase for all the observed mission times. However, when the MTTR = 1 day, we observe that the disconnection probability for mission time of 1 and 2 months are close enough (0.012 and 0.026 respectively). This observation does not hold with increasing values of MTTR. For instance, when MTTR = 7 days, the disconnection probability for all the mission times differs by a larger margin.

We next evaluate the expected Time To Disconnection (TTD) for different MTTR and MTBF values. The expected TTD represents the mean time required to move from the initial state (0:0) with no link failures to the disconnection state in the CTMC. The formalization of this property in CSL is as following:

Property 2: `R{"total_time"}=? [F disconnect]` - "*the mean-time-to-disconnect of the network, i.e. the expected amount of time that elapses before the first disconnection occurs.*"

The obtained results for MTBF of 15, 30, 60 and 180 days are shown in Figures 5. To achieve a target TTD, such analysis can provide hints of what requirements a network operator should demand from the service repair team. For instance, if the MTBF = 30 days and MTTR = 2 days, then the expected TTD is about 50 days approximately. In contrast, if MTTR = 1 day, then the value of MTTD reaches 200 days approximately.

Service unavailability is a major concern for networks that need to maintain high availability. *Service unavailability* represents the average proportion of time in which the network is not available. This can be quantitatively analyzed in PRISM using property 3 and formalized using CSL as following:

Property 3: `(R{"unavailable"}=? [ C<=T ])/T` - "*the expected interval unavailability of the network in the time interval [0, T], i.e. the fraction of that time which it is unavailable.* "

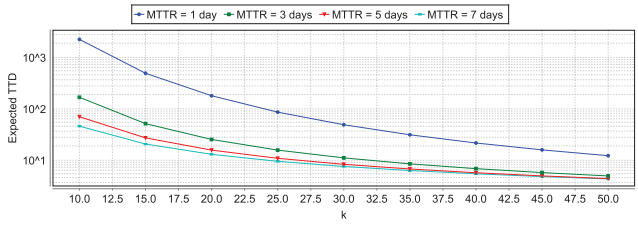

Fig. 7. Expected Time To Disconnection (TDD) for different size of topology with different values of MTTR and MTBF = 60 days

The obtained service unavailability results are shown in Figure 6 for mission time T = 180 days with different values of MTBFs and MTTRs. For instance, if MTBF = 180 days, then *five-nines* (99.999%) availability can be guaranteed only if the MTTR = 1 day. For the same case, if MTTR = 2 days, then *four-nines* availability can be offered.

Next, we analyze the MTTD values for different sizes of k-DRDAs using property 2, but this time for MTBF = 60 days, with different values of k and MTTRs. The results are shown in Figure 7. We observe a decreasing trend of MTTD with respect to k. This is due to the fact that more number of links (a k-DRDA contains $2k$ links) in the topology makes it more failure prone. For instance, a 10-DRDA shows the MTTD of 46 days when MTTR = 7 days. In contrast, a 30-DRDA shows the MTTD of 7.5 days only.

Note that DRDAs provide a high resilience capabilities, which are inversely proportional to its size k. The network operators should consider this critical aspect of DRDAs while designing a given metropolitan area network. Moreover, the inclusion of new nodes in the inner or outer ring to provide more coverage may reduce the total service availability and network operators must provide faster service repair times (i.e., reduce MTTR) as confirmed in reference [17]. The p-cycles based protection mechanism provide effective resilience properties for metro area networks, however, it is not suitable for wide area networks until a reasonable MTTR is guaranteed.

Property 4: `R{"repair"}=? [ C<=T ]` - "*the expected cumulative number of repairs in the time interval [0, T]* "

Property 4 analyzes the expected number of repairs for a mission time of T = 180 days, MTBF = 60 days and different values of MTTRs. The obtained results are shown in Figure 8. Such results can help a network designer to calculate the number of repairs for a given MTBF, MTTR and the mission time. For instance, the figure shows that the repair team will need to perform about 60 repairs when MTTR = 1 day for the mission time of 3 months (note that, the MTBF = 60 days),

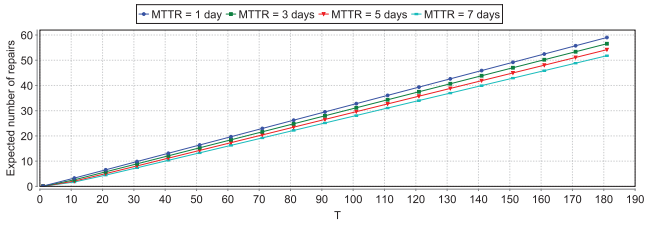

Fig. 8. Expected number of repairs for different MTTRs and MTBF = 60 days and T $\leq$ 6 months

whereas, if MTTR = 7 days then the number of repairs are decreased to 52. Such analysis can be helpful to estimate the repair cost at early network design stages.

These types of automated quantitative analysis presented in this section are particulary handy for multicast services, which demand full-time any-to-any connectivity. A good example of such case can be a IPTV service where a root node transmits signals to all other nodes in the topology. These nodes further transmit the obtained signal to the Digital Subscriber Line Access Multiplexers (DSLAMs) connected to it. The isolation of even a single node due to a failure may cause unexpected disconnection to thousands of subscriber in this case. The PRISM model checker includes multiple model checking engines, many of which are based on symbolic implementations (using binary decision diagrams and their extensions). These engines enable the probabilistic verification of models of up to 10^{10} states. Moreover, the PRISM also features a variety of advanced techniques such as abstraction refinement and symmetry reduction. It is worth mentioning that it also supports approximate/statistical model checking through a discrete event simulation engine. So considering the capability of PRISM model checker, it is also possible to analyze larger models.

V. Conclusion and Future Work

In this work, we presented the formal modeling of Double-Ring topologies with Dual Attachment (DRDA) and also analyzed their dependability when subject to optical link failures. Such a highly-redundant topology is especially practical when the inner nodes and its dual attached outer nodes are close. Indeed the connection of nodes of two rings through dual-attachment results in a less costly solution, which is the case for many metropolitan area networks. The proposed generic Continuous-Time Markov Chain (CTMC) model is able to express the resilience capabilities of a k node network topology with multiple link failures in either of the two dual p-cycles of DRDA. The quantitative results presented in the paper provide some useful insights about the repair rates required to guarantee a certain level of service availability and the evaluation of service availability for different topology sizes. Moreover, we also analyzed the number of expected repairs for a given repair rate subject to a given MTBF and mission time for repair cost estimation.

In classical Markov chains, the transition delay between states are exponentially distributed. However, deterministic intervals can be approximated by inserting multiple intermediate states between every main state pairs which is commonly known as Erlang process [18], [19]. In future, we plan to enrich the model discussed in this paper by adding deterministic repairs and evaluate similar dependability metrics.

References

[1] "MIT's CTR," https://mphotonics.mit.edu/ctr-documents, 2016.

[2] X. Zhou, J. Yu, and M. Huang, "32Tb/s (320x114Gb/s) PDM-RZ-8QAM Transmission over 580km of SMF-28 Ultra-Low-Loss Fiber," in *Optical Fiber Communication Conference and National Fiber Optic Engineers Conference*. Optical Society of America, 2009, p. PDPB4.

[3] R. Ramaswami and K. N. Sivarajan, *Optical Networks - A Practical Perspective*, ser. The Morgan Kaufmann Series in Networking, 2002.

[4] R. Miller, "Hurricane Katrina: Communications and Infrastruc-Ture Impacts," in *Threats at Our Threshold: Homeland Defense and Homeland Security in the New Century*, ser. Eisenhower National Security Series. Optical Society of America, 2007, pp. 191–203.

[5] H. Choi, S. Subramaniam, and H. Choi, "On Double-link Failure Recovery in WDM Optical Networks," in *Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, vol. 2. IEEE, 2002, pp. 808–816.

[6] W. D. Grover and D. Stamatelakis, "Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration," in *International Conference on Communications*. IEEE, 1998, pp. 537–543.

[7] U. Siddique and S. Tahar, "Towards the Formal Analysis of Microresonators Based Photonic Systems," in *IEEE/ACM Design Automation and Test in Europe*, 2014, pp. 1–6.

[8] U. Siddique, V. Aravantinos, and S. Tahar, "Formal Stability Analysis of Optical Resonators," in *NASA Formal Methods*, ser. LNCS, vol. 7871, 2013, pp. 368–382.

[9] C. Baier and J. Katoen, *Principles of Model Checking*. The MIT Press, 2008.

[10] N. Rungta, G. Brat, W. J. Clancey, C. Linde, F. Raimondi, C. Seah, and M. G. Shafto, "Aviation Safety: Modeling and Analyzing Complex Interactions between Humans and Automated Systems," in *Application and Theory of Automation in Command and Control Systems*, 2013, pp. 27–37.

[11] S. Gnesi and T. Margaria, *Practical Applications of Probabilistic Model Checking to Communication Protocols*. Wiley-IEEE Press, 2012, pp. 133–150.

[12] P. S. del Rio, J. Hernandez, J. Aracil, J. L. de Vergara, J. Domzal, R. Wojcik, P. Cholda, K. Wajda, J. F. Palacios, o. Gonzalez de Dios, and R. Duque, "A Reliability Analysis of Double-Ring Topologies with Dual Attachment using p-cycles for Optical Metro Networks," *Computer Networks*, vol. 54, no. 8, pp. 1328 – 1341, 2010, resilient and Survivable networks.

[13] C. Dombrowski, S. Junges, J.-P. Katoen, and J. Gross, "Model-Checking Assisted Protocol Design for Ultra-Reliable Low-Latency Wireless Networks," in *Symposium on Reliable Distributed Systems (SRDS)*. IEEE, 2016, pp. 1–10 (To Appear).

[14] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM 4.0: verification of probabilistic real-time systems," in *Computer aided verification*. Springer, 2011, pp. 585–591.

[15] H. Hansson and B. Jonsson, "A logic for reasoning about time and reliability," *Formal Aspects of Computing*, vol. 6, no. 5, pp. 512–535, 1994. [Online]. Available: http://dx.doi.org/10.1007/BF01211866

[16] C. Baier, J.-P. Katoen, and H. Hermanns, "Approximate symbolic model checking of continuous-time markov chains (extended abstract)," 1999.

[17] P. Cholda and A. Jajszczyk, "Reliability Assessment of Optical P-cycles," *IEEE/ACM Transactions on Networking (TON)*, vol. 15, no. 6, pp. 1579–1592, 2007.

[18] K. A. Hoque, O. A. Mohamed, and Y. Savaria, "Towards An Accurate Reliability, Availability and Maintainability Analysis Approach for Satellite Systems Based on Probabilistic Model Checking," in *Design, Automation, and Test in Europe*. IEEE, 2015.

[19] K. A. Hoque, O. A. Mohamed, Y. Savaria, and C. Thibeault, "Probabilistic Model Checking Based DAL Analysis to Optimize a Combined TMR-Blind-Scrubbing Mitigation Technique for FPGA-Based Aerospace Applications," in *International Conference on Formal Methods and Models for Co-Design*. ACM-IEEE, 2014.