Software tool for network reliability and availability analysis

Gerardo Castañón[1], Ana Maria Sarmiento[2], Raúl Ramírez[3], and Alejandro Aragón-Zavala[4].

[1]Center of Electronics and Telecommunications,
[2]Department of Industrial Enginering,
[3]Department of Electrical Engineering
Tecnológico de Monterrey
Eugenio Garza Sada 2501 Sur, Monterrey, N.L., 64849, México
[1]e-mail:gerardo.castanon@itesm.mx,

[4]Center of Information Technologies, Tecnológico de Monterrey
Campus Querétaro, Querétaro, Qro., México.

Abstract

The emerging communication applications such as IPTV, VoIP, infotainment, interactive games, and Internet access might dictate very high reliability and availability in future fiber access networks. We present an easy-to-use software tool, called *NetExpert*, designed to simplify the network planning, design and optimization processes and save valuable time preparing network configurations that provide a desired level of network reliability, availability, and fiber length. The reliability and availability model used in the software tool is presented in the paper. We present a comparative analysis of network topologies for Fiber Networks. In particular, we present results that compare different topologies such as as star, ring, bus, multilevel stars, multilevel rings, multilevel buses, hybrid multilevel star-rings, hybrid multilevel ring-stars, and hybrid multilevel ring-buses in terms of availability, reliability, and fiber length requirements of networks. Protection is also considered and results on the protected versions of the aforementioned topologies are also presented.

1. Introduction

It is a well known fact that the use of software applications for the design, analysis and optimization of different systems enables people to efficiently and timely perform the tasks needed. Communication networks are no exception and software applications to support their design and optimization are of most importance to companies and individuals in the Telecommunications industry. Through the use of these software tools, different scenarios can be created and analyzed by the network planner saving valuable time and effort. The software application presented in this paper has been developed with these requirements in mind. Three of the most important parameters in the design of a communication network are its reliability, availability and fiber length required. The software tool presented in this paper, *NetExpert*, accounts for all such parameters and many more. The algorithms imbedded in the software are amidst the most efficient that exist in the literature up to this day. We present a high level description of these algorithms for the reliability and availability of networks and present examples of network scenarios in which the tool is used. We also present a comparison of different topologies for fiber networks, highlighting the usability of the software tool and its benefits. The remainder of this paper is as follows; in Section 2 we present a summary of the relevance of fiber networks in today's competitive communication environments specifying the existing needs for optimization. Section 3 presents the description of the algorithms regarding reliability and availability imbedded in the software tool *NetExpert*. Section 4 provides an overall view of the software tool itself. Section 5 presents the comparison of different topologies for fiber networks considering protection schemes and Section 6 presents the conclusions.

2. Communication Networks

In today's communications-focused market, affordable, reliable communication is integral to staying competitive with a fast-paced marketplace. Large companies spend hundreds of thousands of dollars to maintain and grow computer networks, phone systems, call centers, voice mail services and video conferencing. Even small and entrepreneur companies invest in their communication networks. In other applications, there is also an increasing interest in road accident prevention, radar vehicular technology, and traffic congestion in intelligent transportation systems, which require secure and reliable network infrastructures. For all these applications it is necessary to perform analyses that lead to the design of networks that have high reliability and availability. Without them, networks will be confined to limited environments, not fulfilling much of the promise they hold. As shown in Figure 1 [1], fiber network topologies investigated in this paper can be used for wireless services as well as for fiber to the home and fiber to the building services. Due to the vast bandwidth of the fiber, both wireless and wired services in a single fiber access network can co-exist. However, this will require network planning to distribute the bandwidth for both services according to the traffic and demand requirements.

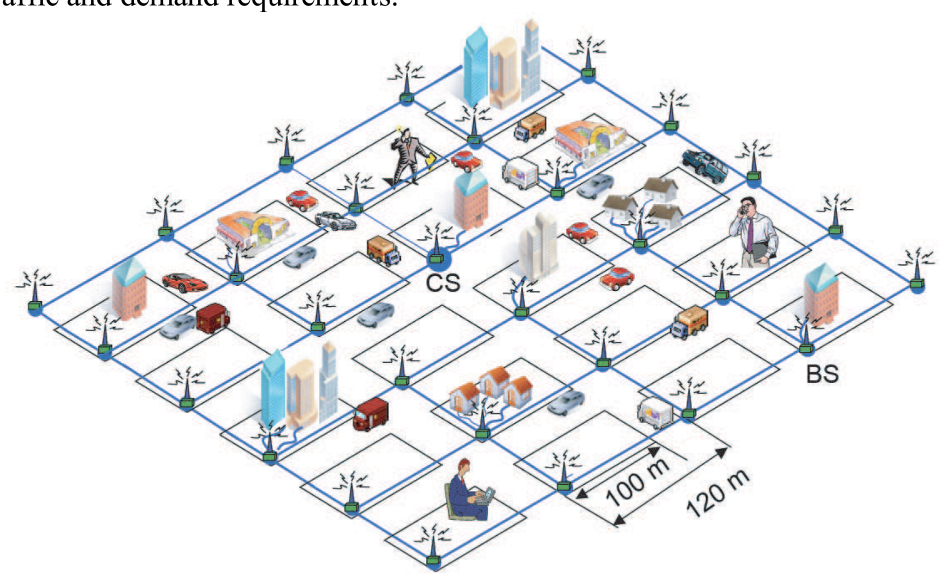


Fig. 1. The envisioned network in urban areas. Radio over fiber for vehicular, mobile, broadband wireless computer communications and also network infrastructure can be used for fiber to the building and fiber to the home services.

Without proper security and reliability mechanisms, networks will be confined to limited, controlled environments, not fulfilling much of the promise they hold. The limited ability of Vehicular/Mobile/Wireless/Computer networks to thwart failures or attacks makes ensuring network availability more important and difficult. Consideration of security, reliability, and availability at the design stage is the best way to ensure successful network deployment.

Computer applications can substantially aid in the design of communication networks by providing a means to tryout different scenarios with multiple considerations. Furthermore, future networks will be composed by thousands of interconnected network components and tools, making the quantification of the reliability and availability of communications extremely important. The quality of the results obtained by these tools will clearly depend on the type of optimization the software tool performs, for this reason the algorithms imbedded in the tool should be reliable in order to assure optimal results.

3. Reliability and Availability in networks

Reliability is a key parameter in the design of highly reliable communication networks. In essence, reliability indicates the quality of the network to transport traffic. Thus, reliability is a probability measure and is defined as the probability that there exists one operative path between a given pair of communicating entities. Network reliability is a classical problem and has been studied extensively by many researchers in the past [2-12]. The software application *NetExpert* uses the algorithm SYREL [11-12] to compute reliability; this algorithm is accurate and has a relatively low computational complexity.

SYREL [12] algorithm incorporates the best features of both path and cutset methods. Algorithms based on path and cutset enumeration with reduction to mutually exclusive events are generally efficient and produce compact expressions. In path (cutset) enumeration methods, the entity reliability (unreliability) expression is obtained by finding the set of possible paths (cutsets) between a pair of entity nodes and then applying Boolean algebra and probability theory to modify the set of paths (cutsets) to an equivalent set of mutually exclusive paths. The entity reliability (unreliability) expression can then be obtained in a straightforward manner from the disjoint set of paths (cutsets).

The SYREL algorithm starts by representing communication entities as nodes and the communication links between them as edges on a graph. The algorithm assumes that the failures of elements are statistically independent and the probability of an element being up (or down) is considered. An expression for entity reliability R between a pair of nodes is obtained as

$$R = P_r\left(\bigcup_{i=1}^{m} E_i\right) \tag{1}$$

where E_i denotes the event in which path P_i is up and m represents the number of paths between those two nodes. This expression for the entity reliability can be computed by decomposing the set of paths in the graph into another set of mutually exclusive paths between two nodes.

Equation (1) is then decomposed into mutually exclusive events that consider all possible cases of paths being operational or not operational between a pair of nodes, and then written in terms of conditional probabilities of the aforementioned events. Hence the terminal reliability expression can be evaluated in terms of two distinct events. The first event indicates that a path, say P_i, is in the operational state while the second event indicates that all the previous paths, which are $P_1, \cdots, P_{i-1}$, are in the failure state, conditional to P_i being operational. The SYREL algorithm efficiently computes the probabilities for these two events.

The *availability* of service is also an important issue in today's networks. In the case of a link or node's component failure, several communication connections will be affected. To guarantee a desired level of communication service availability, the network must be analyzed in an integrated manner. The calculation of availability in the software application *NetExpert* is done through the availability maps [1,13,14] that are a function of the connection length and of the number of traversed nodes. They provide results to visualize the combined influence of node and link failures on the connection availability in a network. The connection availability is calculated by the following equation [1,13]:

$$A_c = 1 - \begin{pmatrix} AP_{link-km} D + AP_{drop} + AP_{add} + AP_{pass-through} ceil((H-1)(1-P_{reg})) \\ + AP_{reg} floor((H-1)P_{reg}) \end{pmatrix} \tag{2}$$

where $AP_{link-km}$ is the link availability penalty per kilometer, D is the connection distance in kilometers, H is the number of hops traversed by the connection, $AP_{add}, AP_{drop}, AP_{pass-trough}$, and AP_{reg} are the availability penalties due to adding, dropping, passing through, and regeneration node operations, respectively. P_{reg} is the fraction of nodes in which the connection is regenerated. The functions ceil(x) and floor(x) are the ceiling and floor functions, respectively.

In general, the availability penalty imposed by a system can be derived from its failure rate (FR) in FIT (1 FIT = failure rate of 1 failure in 10^9 hrs) by the following equation:

$$\mathrm{AP} = 10^{-9} * \mathrm{FR} * \mathrm{MTTR} \tag{3}$$

where MTTR is the mean time to repair (in hours). This paper assumes a link failure rate of 310 FIT/km [13]. Here we do not consider Raman-pumped amplifiers and we only consider optical Erbium doped fiber amplifiers (EDFAs). The link MTTR was assumed to be 12 hrs and the node components MTTR is assumed to be 6 hrs [13]. These values may vary from operator to operator; nevertheless, this assumption does not have a strong impact on the quantitative availability results.

The architecture of a node is shown in Fig. 2. It is based on passive components splitters/couplers, filters, wavelength blockers, and optical amplifiers to compensate for loss when it is required. Node operations are also shown in Fig. 2. The signal can pass through the node, can be dropped and a new signal can be added. The block diagram used for calculating the availability penalty of each node operation is shown in Fig. 3 which also shows the components involved in case the signal needs to be regenerated.

Table 1 contains some common component failure rates used in the design of optical networks [13]. The needed values are substituted in equation 2 to calculate node operations according to Fig. 4 and the penalties calculated are substituted into equation 1 to compute the connection availability.

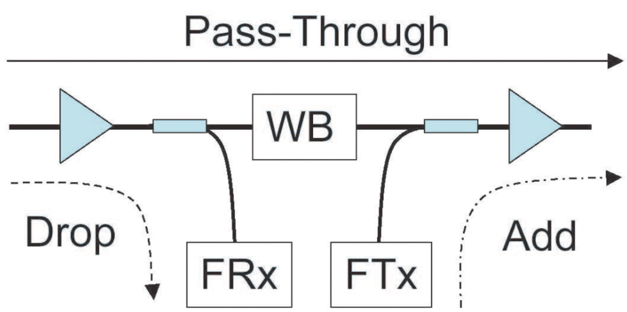


Fig. 2. OADM architecture. Node operations are: passing through (solid line), dropping (dashed line), and adding (dashed-dotted line).

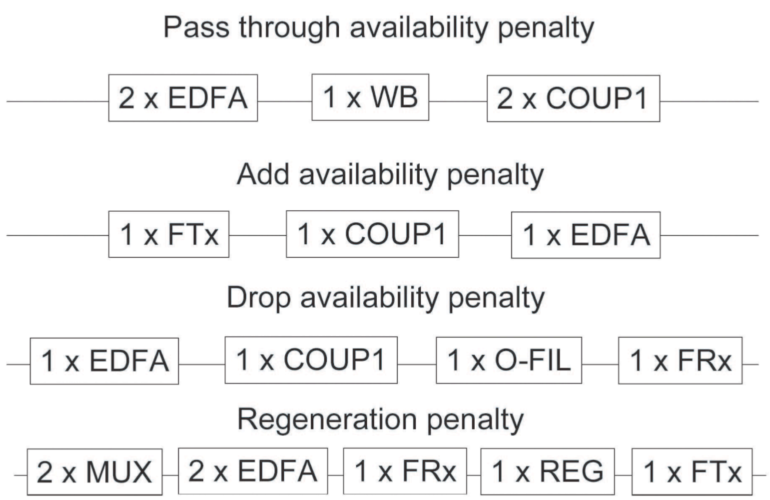


Fig. 3. OADM block diagrams of the availability penalties.

Table 1. COMPONENT FAILURE RATES.

Component	*Symbol*	*Failure Rate (FIT)*
Number of wavelengths	W	
Number of inputs	N	
MUX/DEMUX	MUX	25 * W
EDFA	EDFA	2850
Optical Switch 1	OSW1	21 * W * W/4
Optical Switch 2	OSW2	21 * 2 * 2N
Coupler 1	COUP1	50
Coupler 2	COUP2	25* W/4
Coupler 3	COUP3	25*(N-1)
Tunable Transmitter	TTx	745
Fix Transmitter	FTx	186
Tunable Receiver	TRx	470
Fix Receiver	FRx	70
Digital Switch 1	DSW1	875* W
Digital Switch 2	DSW2	875* W *N
Wavelength Blocker	WB	50 * W

4. NetExpert Network Planner.

NetExpert Network Planner is an easy-to-use software tool designed to simplify the network planning, design and optimization processes and save valuable time preparing network configurations.

With the introduction of new network technologies such as Metro Ethernet, IP, VoIP, and Optical Mesh, as well as new triple play services, communications service providers (CSPs) must invest heavily in network and service infrastructure. Designed to help manage the uncertainties and risks associated with these investments, NetExpert is a modern network resource planning system. With NetExpert, CSPs have a single, cross-domain network resource planning system across all network layers. NetExpert provides specific and quantitative answers to the decision-making processes associated with network planning and resource management. It captures network information across all layers and stores this information in a single repository, NetExpert provides a platform to act as the common network resource planning application. In short, NetExpert modernizes a CSP's network infrastructure to accommodate new services and reach out to new customers. At the same time, NetExpert cuts capital and operational expenditures for CSPs competing in the next network generation environment.

Figure 4 presents a screen view of one of NetExpert's interfaces for the availability, reliability and fiber distance analyzers. For each one of these analyzers, a window pops up presenting all the parameters the planner can input into the tool to test different scenarios, for example the availability analyzer contains 4 submenus to input information about failure rate, analysis options, link options and node/link information. Similar capabilities are found in the different analyzers in NetExpert. To learn about all the functionalities of NetExpert visit www.whitepaths.com.

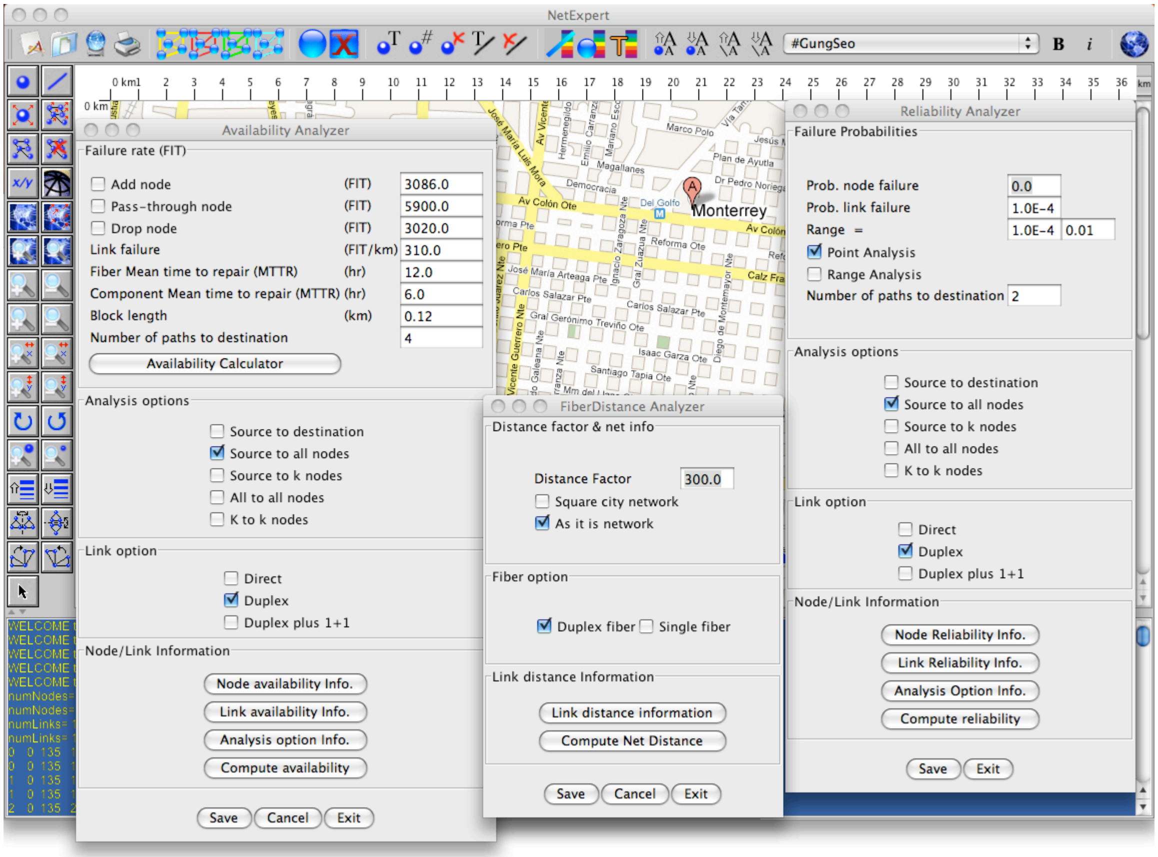


Fig. 4. NetExpert: availability, reliability and fiber distance analyzers.

5. Network examples and analysis

Figure 5, shows topologies with 25 nodes where Fig. 2a is a star, Fig. 2b is a ring, Fig. 2c is a bus Fig. 2d multilevel stars, Fig. 2e is a multilevel rings, Fig. 2f is a multilevel buses, Fig. 2g is a multilevel star-rings, Fig. 2h is a multilevel ring-stars, and Fig. 2i is a multilevel ring-buses topology. The separation between nodes used in this paper is 120 meters considering that the typical average length of a street block in large cities is 100 meters. We will assume that each base station is at the corner of every street intersection in a rectangular grid of streets. The reliability and availability calculations consider the reference distance of 120 meters between base stations. Now, the number of wavelengths in a fiber link depends on the number of nodes that a given link is interconnecting to the central station. In this paper we are limiting the reliability and availability analysis to the case of considering the probability that the central node communicates with the other nodes of the network.

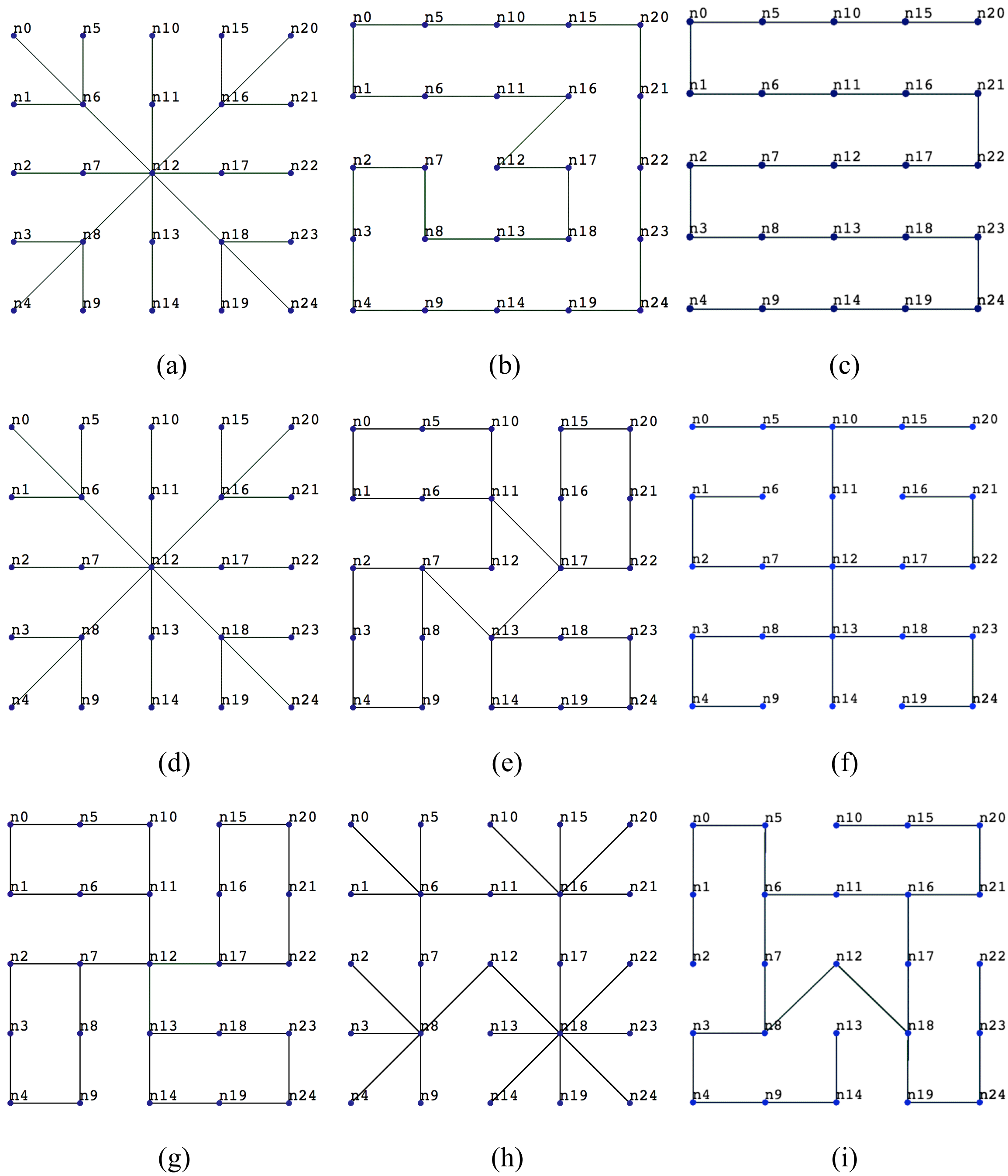
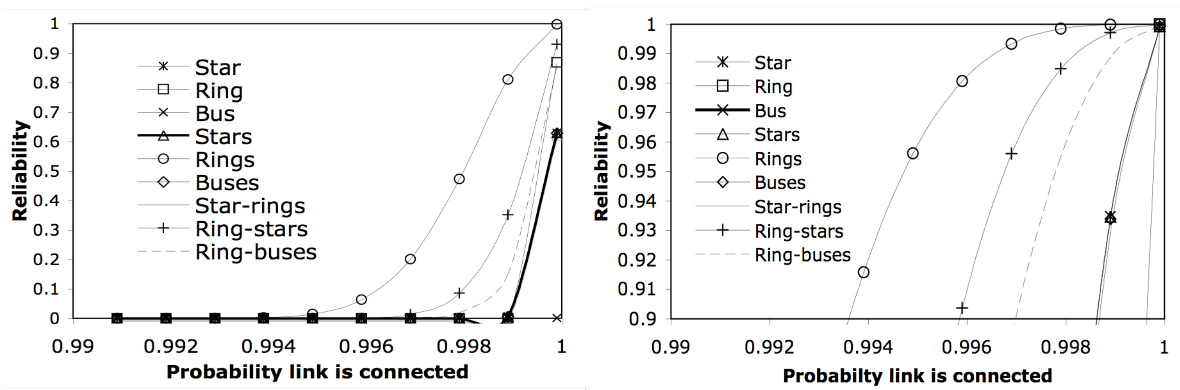


Figure 5. Topologies a) star, b) ring, c) bus, d) multilevel stars (stars), e) multilevel rings (rings), f) multilevel buses (buses) g) multilevel star-rings, h) multilevel ring-stars, and i) multilevel ring-buses.

The results presented consider the probability that the central node communicates with the other nodes of the network. Considering Figure 5, the central node is located at node number 12. Reliability is computed in this way because it is assumed that the central station is communicating with all the nodes and all nodes with each through the central node. One important feature about the analysis presented in this paper is that it considers the probability of link failure as link length dependent. For example, if the probability a link of length 120 meters does not fail is ρ, then the probability that a link of length 900 meters does not fail is $\rho^{(900/120)}$. This makes the reliability analysis of the topologies length dependent, link failure parameter dependent, and number of paths (source-destination) dependent, which emulates what happens in reality in an effective manner.

Figure 6, shows results of the network reliability for cases with 441 nodes. Fig. 6 (a) is for the case of no protection scheme and (b) shows results for the case when 1+1 protection is used in the topologies. We are assuming a 1+1 protection scheme because it increases network reliability. For the 1+1 protection case we assumed redundant disjoint fiber links are installed. The link disjoint path protection is the one where the working link and the protection link are physically separated from each other. The physical separation of the working path and protection path may be implemented by installing them in separate ducts, if the fiber is installed underground or installing the fiber in separate electric poles if the fiber is installed over ground. The impact of considering this in the reliability and availability analysis is that the link failure of the working path is an independent variable with respect to the link failure variable of the protection path.



(a) (b)

Fig. 6. Reliability against probability link is connected for multilevel-rings and multilevel ring-stars topologies considering 441 nodes. (a) is for the case of no protection and (b) is for the case of 1+1 protection.

To compute the results in Figures 6 we assumed link failure only. The probability a link of length L (meters) is working, i.e. the probability a link of length L remains without failure ρ, has a range from 0.99 to 0.9999. It is important to note that L here denotes the basic length unit. In this paper, we consider the separation L between BSs equals to 120 m, assuming that 100 m is the average length of a typical block in a city as shown in Figure 1. It is important to note that the multilevel-rings topology referred to in Figure 6 as rings provides the best reliability performance for networks with 441 nodes without protection and also when 1+1 protection is used.

Figure7 shows fiber length of topologies similar to the topologies shown in Figure 5. Figure 7 shows results for networks without protection with 25, 49, 121, 441, and 1089 nodes. If 1+1 protection is considered, the amount of fiber length will double. It is important to note that results in Fig. 7 show the total amount of fiber length in the network and not the maximum distance from the central node to the farthest node. The networks were designed using the same logic of interconnection of the nodes as in Fig. 5. Note that the topology with the lowest link length values is the ring topology.

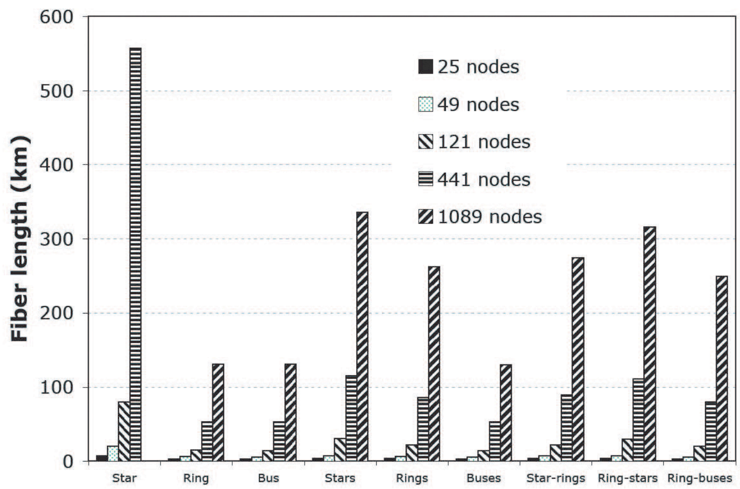


Fig. 7. Fiber length in kilometers against number of nodes for networks without protection.

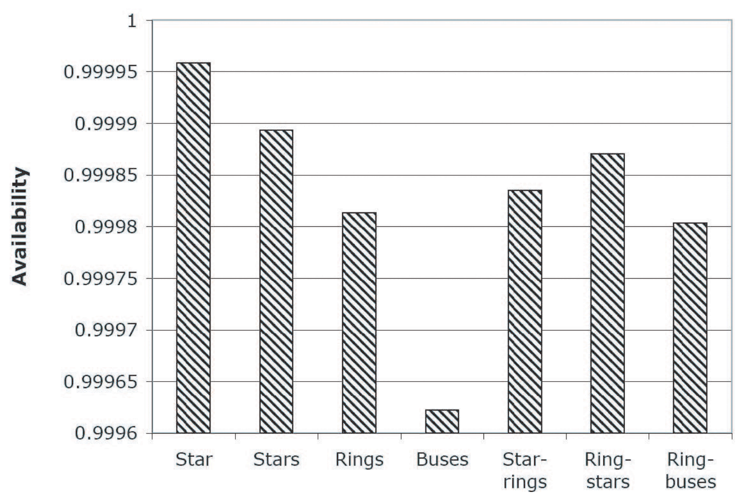
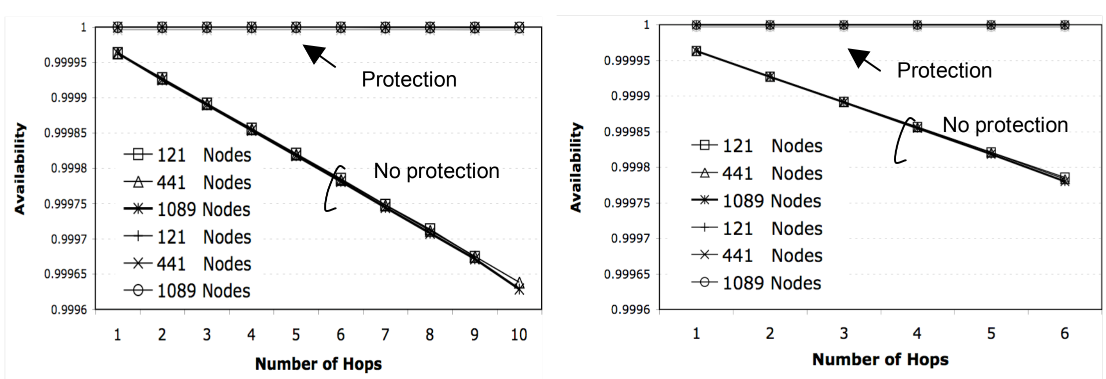


Fig. 8. Availability of star, multilevel stars, multilevel rings, multilevel buses, multilevel star-rings, multilevel ring-stars, and multilevel ring-buses, topologies for networks with 441 nodes without protection.

Results of average network availability are shown in Fig. 8 for networks without protection and with 441 nodes. For the case of the multilevel-rings we used 10 nodes per internal ring and 10 nodes per outer ring and for the case of the multilevel ring-stars we used 10 nodes per internal ring and 10 nodes per outer star. Also, for the case of multilevel ring-buses we used 10 nodes per internal ring and 5 nodes per outer bus. The internal rings are the ones that interconnect the central node with one node of the outer rings/stars/buses. Note in Fig. 8 that the star topology yields the highest availability performance at the expense of requiring a large fiber length.

In order to provide more insight into the network availability performance we present results of network availability versus number of hops in Fig. 9. Results are for the multilevel rings and for the multilevel ring-stars topologies with 121, 441, and 1089 nodes for the unprotected and protected schemes. Fig. 9 presents results of availability against number of hops. For the multilevel-rings topologies we used 10 nodes per internal ring and 10 nodes per outer ring and for the multilevel ring-stars topologies we used 10 nodes per internal ring and 10 nodes per outer star. The internal rings are the ones that interconnect the central node with one node of the outer rings/stars. Note that in a square node location multilevel-rings network with 121 nodes, the maximum number of hops is 9. If the network contains 441 or 1089 nodes the maximum number of hops is 10. Observe also that for the multilevel ring-stars topology the maximum number of hops is 6 independently of the number of nodes in the network. The multilevel ring-stars topology has the advantage of requiring a lower number of hops to reach the nodes compared to the multilevel-rings topology. Also, the multilevel ring-stars topology has the advantage that it is relatively easy to "grow" when a new node is required in a certain location. Availability results are an average of the availability of nodes that have the same number of hops to and from the central node. We quantify the availability parameter from the central node to all the other nodes and then we compute the availability average among all the nodes that have the same number of hops from the central node. Note that the availability for the unprotected case becomes worse with the number of hops and the availability is lower than the 'five nines' standard for both topologies. If the network is protected with the 1+1 scheme the availability improves considerably and results are greater (i. e., better) than the 'five nines' (0.99999) standard of network availability for both topologies.



(a) (b)

Fig. 9. Availability against number of hops for a) multilevel-rings and b) multilevel ring-stars topologies for networks with and without protection with 121 nodes, 441 nodes, and 1089 nodes.

6. Conclusions

We present an easy-to-use software tool, called *NetExpert*, designed to simplify the network planning, design and optimization processes and save valuable time preparing network configurations that provide a desired level of network reliability, availability, and fiber length. The reliability and availability model used in the software tool is presented in the paper. We present a comparative analysis of network topologies for Fiber Networks. In particular, we present results that compare different topologies such as multilevel rings and multilevel ring-stars in terms of availability, reliability, and fiber length requirements of networks. Protection is also considered and results on the protected versions of the aforementioned topologies are also presented. Considering the three parameters in the comparison, it turns out that the multilevel rings and multilevel ring-stars achieve the best overall results. However, multilevel ring-stars topology is interesting from the point of view that it is relatively easy to "grow" when a new node is required in a certain location. The network availability results presented show that in order to fulfill the 'five nines' availability standard the networks must have a protection scheme. The 1+1 link disjoint protection scheme analyzed in this paper yields availability results superior to the '*five nines*' standard. Other protection schemes may be analyzed using the methodology presented in this paper in order to compare availability and cost reduction of a specific protection scheme. For all these analyses, NetExpert provides an excellent tool for the design of different network configurations, making the comparison of different topologies accessible and more efficient.

References

1. Gerardo Castañón, Gabriel Campuzano, Ozan Tonguz, "High reliability and availability in radio over fiber networks", OSA Journal of Optical Networking, Vol. 7, No. 6, pp. 603-616, June 2008.
2. Charles J. Colbourn. *The Combinatorics of Network Reliability.* Oxford University Press, New York, 1987.
3. A. M. Shooman, "Algorithms for Network Reliability and Connection Availability Analysis", IEEE, pp. 309-333, April 1995
4. Y. F. Lam and Victor 0. K. Li. "An improved algorithm for performance analysis of networks with unreliable components", *IEEE Transactions on Communications,* COM-34(5): pp. 496-497, May 1986.
5. A. M. Shooman. *Exact Graph-Reduction Algorithms for Network Reliability Analysis.* PhD thesis, Polytechnic University, Brooklyn, New York, June 1992.
6. A. M. Shooman and Aaron Kershenbaum. "Exact graph-reduction algorithms for network reliability analysis" In IEEE *GLOBECOM '91 Proceedings,* pp. 1412-1420, December 1991.
7. Kin-Ping Hui, "Network Reliability Estimation" PhD Thesis, The University of Adelaide Faculty of Engineering, Computer and Mathematical Sciences, 2005.
8. M.L. Shooman, E. Cortes, "Reliability and Availabillity Modeling of Coupled Communication Networks ASimplified Modeling Approach", In proceedings Annual Reliability and Maintability Symposium, Vol. 1. pp. 129-136, 1991.

9. A. M. Johnson, M. Malek, “Survey of Software Tools for Evaluating Reliability, Availability, and Serviceability”, ACM Computing Surveys, Vol. 20, No. 4, pp. 227-269, December 1988.
10. Soh, S. Rai, “CAREL: Computer Aided Reliability Evaluator for Distributed Computing Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 2, No. 2, pp. 199-213, April 1991.
11. S. Hariri and C. S. Raghavendra, “SYREL: a symbolic reliability algorithm based on path and cutset methods,” IEEE Trans. Comput. **C-36**, pp.1224–1232 (1987).
12. C. S. Raghavendra, V. K. Prasanna Kumar, and S. Hariri, “Reliability analysis in distributed systems,” IEEE Trans. Comput. **37**, 352–358 (1988).
13. D. A. A. Mello, D. A. Schupke, and H.Waldman, “A matrix-based analytical approach to connection unavailability estimation in shared backup path protection”, IEEE Photonics Technology Letters, vol. 9, pp. 844-846, September 2005.
14. D. A. A. Mello, D. A. Schupket, M. Scheffelt, and H. Waldman, “Availability maps for connections in WDM optical networks”, Proceedings of the 5th International Workshop on Design of Reliable Communication Networks (DRCN), vol. 1, pp. 77-84, October 2005.