Military Technical College
Kobry El-Kobba
Cairo, Egypt

12-th International Conference
on
Aerospace Sciences &
Aviation Technology

AVAILABILITY CALCULATIONS FOR A PROPOSED EGYPTIAN LONG-HAUL NETWORK USING NETWORK PERFORMANCE EVALUATION MODELLING

Dr. Wafae Bogdady[1], Dr. Atalla I. Hashad[2], Eng. Dalia M. Elgamel[3]
1 National Telecommunication Institute, 2, and 3 Collage of Engineering, Arab Academy for Science & Technology Cairo, Egypt.

ABSTRACT
The incoming new generation network has three main objectives to be achieved: (1) Quality of Service (QoS) which is controlled by the bit error rate (BER), congestion rate, the latency, and the throughput. (2)Reliability controlled by the network availability & survivability. (3) Security controlled by the wide spread use of incriptian, the access control, the authentication & authorization, auditing or accounting. Network availability models are built, where the networks Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) are measured depending upon the components types, and the failure rates of optical cable. Mesh architecture is proposed, and analyzed to increase the availability of the Egyptian backbone when applying the span protection, and path protection method on this architecture.

KEYWORDS: Core networks, Protection technique, availability, graph theory.

1. INTRODUCTION
High availability of the telecommunication services has traditionally been expected and is being equally important for end users and contracted services providers. The importance of network availability grows with steadily increase of the network capacity; next generation optical networks will provide the pathways to transport, potentially, terabits of data. Network reliability and protection are among the most important issues concerning the transport of high-speed connections: interruption of an optical connection even for a short period could cause the loss of a huge quantity of data (e.g. 5 GByte for 40 Gbit/s modulated wavelength channel) [1], failures happen quite frequently and with catastrophic consequences. The impact of the network outage can be normally measured in terms of customer-minutes. Outage can be normally multiplied by the number of affected customers.
Today's telecommunication industry much effort is put into the increase of infrastructure. We take that into consideration. This paper studies the network availability optimization and gives guidance to network operators on how to increase the QoS. To survive today's marketplace, operators must run efficient, network availability optimization to make investment and repair strategy with respect to their Service Level of Agreement, (SLA). As part of SLA the network operator commits certain availability for a connection. Common requirements are that a connection

should be available 99% to 99.999% (five 9s) of the time. Five 9s corresponds to a connection downtime of 5 minutes per year. In order to achieve high service availability networks are designed survivable, they are able to continue providing service in the case of failure. They are using a pre-assigned or dynamically assigned spare capacity within the network enabling the rerouting of the affected traffic around the failure. Networks are commonly designed for 100% protection or restoration if a single failure is occurring to any span or path, this can be handled but node failures are not considered. This may lead to 100% protection or restoration for a single failure but not for multiple failures [2].

Failures in an optical network can be distinguished whether they are damage links or switching devices. In the first situation, faults often results from external causes: cable cuts are very frequent especially in the terrestrial networks since fiber cables often share other utility transport conduits, such as gas or water pipes and electrical cables. Equipment failures in the network nodes are mainly due to internal causes, such as hardware degradation or management software inefficiency. They can result also from exceptional events such as natural phenomena, power block outs. As in the report of the U.S. during1997, there are 136 cuts per year, so, it is irrelevant in some places to take the optical cuts only, we have to take into consideration the equipments, some authors mentioned that equipment failures are proved to be less common on average than transmission links failures: so in our study we will compare between links failures and equipments failure. Availability calculations to demonstrate which area needs to be protected according to the digging-up, also according to the topology of the network, whether they are ring or mesh, because for many years, ring and mesh architecture have been considered by operators for their networks. In the study of network architecture vulnerability (Survivability), it was found that mesh architecture is more robust than two rings connected to each other, for a single ring and star whatever is the number of nodes [4]. Rings can restore failures fast in (50-60ms), with at least 100% extra capacity where this figure is only 50-70% (depending on the network topology) for meshes. In this paper, we deal with Optical Transport Networks (OTNs), availability calculations using span protection, & path protection technique. The software is used to enhance the availability of a network according to its topology, using graph theory algorithms. The availability which we refer to is the classical reliability theory [5]; also, the network design based on static traffic matrix.

2. a. Reliability & Availability

The theory of reliability and availability analyzes the system based on a set of distinct subsystems, connected to obtain an intended function. Reliability (R) is defined as the probability that a system will perform its intended function for a specified period of time under a given set of conditions. Availability (A) inherently reflects a statistical equilibrium between failure process and repair process in maintained repairable systems that are returned to the operating state following any failure. Roughly, availability may be viewed as the fraction of time that a system is in an operational state independently of how many times it was previously broken and repaired. So, if we may assume that systems component, and subsystems are not repairable, we will refer to reliability, while the availability is a typical feature of restorable systems.

Reliability theory, gives the instruments to calculate the reliability parameters of a complex system [2]. The starting point of such evaluation is availability characterization of the system functional blocks, so, any system functional block can

be associated to an instantaneous rate of failure z (t), parameters of this model are commonly specified by technology vendors or may be identified by experimental testing before system installation and then may be updated by field measurements during the system operating lifetime.

Any availability analysis is based on reliability data, i.e. failures rate λ and repair rates μ of the involved equipment. This modal is based on the usual approximation of considering a constant failure rate z (t) = λ, corresponding to a negative exponential reliability function R (t) $=e^{-\lambda t}$. According to such approximation, the mean time to failure MTTF=1/ λ, and mean time to repair MTTR=1/ μ, also we introduce the mean time between failures (MTBF) parameter, which is given by MTBF=MTTF+MTTR. When failure free operating times and repair times are exponentially distributed [1], [3]. Since, we can call the links as a repairable links, and the system availability A, we can call its parameter as the average outage time.

$$A = \frac{MTBF}{MTBF + MTTR} \tag{1}$$

And it's complementary as the unavailability of a system

$$U = 1 - A$$

To calculate the availability we have to model the network by the Reliability Block Diagram (RBD), as shown in figure (2. b, 3. b)

2. b. Protection strategies

There are several approaches to ensure fiber network survivability. Survivable network architectures are based either on dedicated resources or on dynamic restoration as shown in fig (2). In dedicated-resource protection (which includes automatic protection switching (APS) or self-healing rings), the network resources may be dedicated for each failure scenario, or the network resources may be shared among different failure scenarios. In dynamic restoration, the spare capacity available within the network is utilized for restoring services affected by a failure. Generally, dynamic restoration schemes are more efficient in utilizing capacity due to the multiplexing of the spare-capacity requirements and provide resilience against different kinds of failures, while dedicated-resource protection schemes have a faster restoration time and provide guarantees on the restoration ability.

Path-protection is the mechanism that automatically switches the traffic from the working path to a predetermined and diverse path connecting start and end node in case of span or node failure. Path protection can be implemented as 1+1, 1;1, or 1:N. In the case 1+1 traffic is transmitted simultaneously on both path, but one path is selected for transmission usually based on the quality of the signals.

Span-protection a failed span is bridged by a backup path whose start and end nodes is the adjacent to the failed span. In contrast to path protection it is implicitly assumed no redundant path can be established in the case of node failure.

Shared-Protection is the mechanism that in shared-path protection, the resources along a backup path may be shared with other backup paths. As a result, backup channels are multiplexed among different failure scenarios (which are not

expected to occur simultaneously), and therefore, shared-path protection is more capacity efficient when compared with dedicated-path protection.

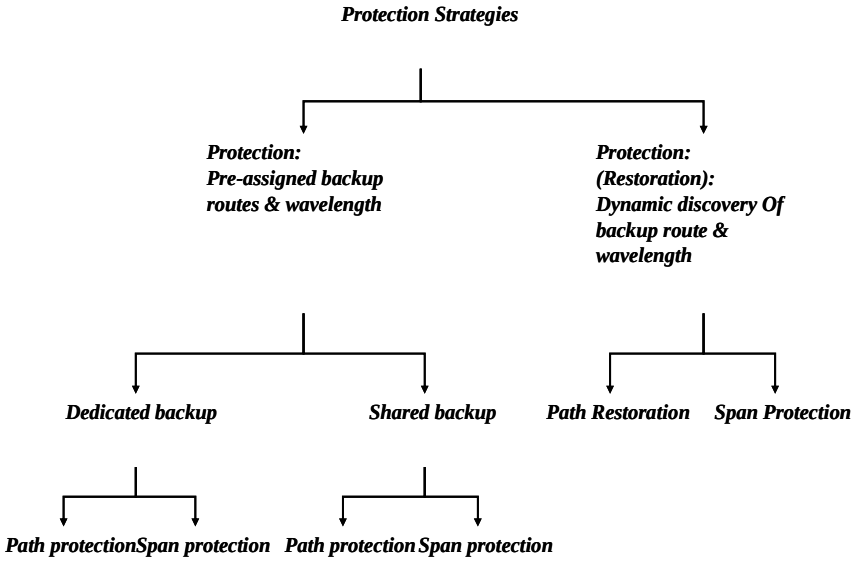

Fig. 1 Different schemes for path protection and restoration

Protection-cycles This a Special case of shared protection is the protection cycle (P-cycle) strategy introduced by Gover [6]. As in span protection a failed span is bridged by a backup path whose start and end nodes are the nodes adjacent to the failed span.

Path-restoration In path restoration, the source and destination nodes of each connection traversing the failed link participate in a distributed algorithm to dynamically discover an end-to-end backup route. If no routes are available for a broken connection, then the connection is dropped, as shown in Fig (2).

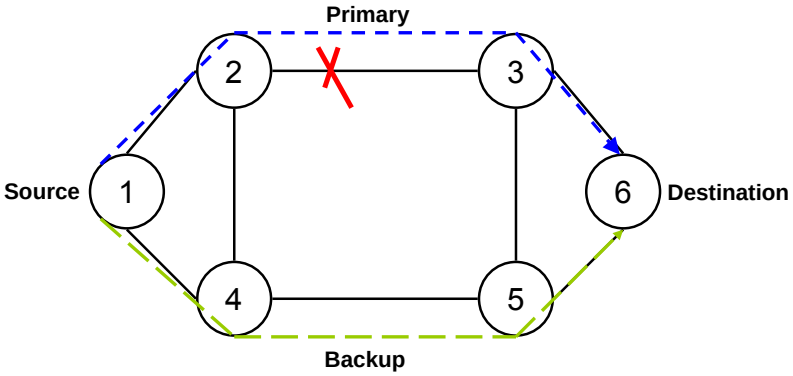

Fig. 2. a **.** *Path protection.*

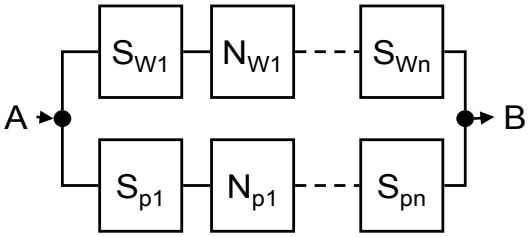

Fig. 2. *b. RBD of path protection*

Span –restoration In Span–restoration the end nodes of the failed span dynamically discover a route around the link as shown in Fig.(3), all the connections that traverse the failed span are rerouted around that span [7].
So the basic condition of end-to-end protection is working and protecting lightpaths being routed along failure independent network. Given that nodes have been assumed with no failure as failure happens according to catastrophic events, also given that with the link-disjoint (the path from the source to destination won't share its protection , fig(3)), it will give absence in failure correlation between any source and destination. So, we can calculate the working path availability independent form its protection.

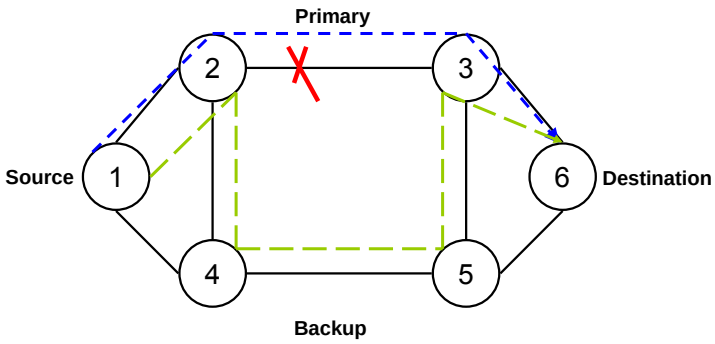

Fig. 3 .a Span restoration network.

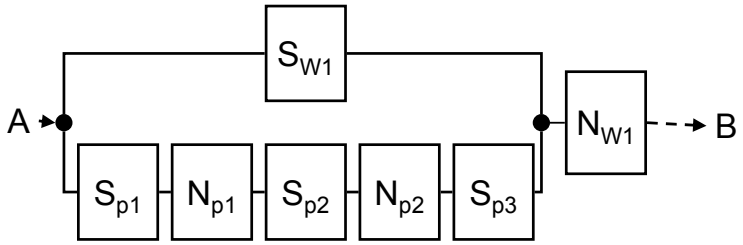

Fig. 3 . b RBD of span restoration.

3. Design procedure

The network is modeled by directed (digraphs) graph, whose vertices represent the network switching nodes and whose directed edges represent the transmission fibers. All networks considered have a pair of unidirectional working fibers (constituting a bidirectional working span) and a pair of unidirectional protection fibers (constituting a bidirectional protection span).

The program developed using C language used for simulating the model, and the minimum- weight path-searching algorithm, or Dijkstra algorithm to find the highest unavailability along the whole network, so the search can define the weakest points on it to show how to give the maximum protection for it. Also, the program has Breadth-First –Search algorithm to find alternate paths when a single cut happens, according to the remaining capacity.

Table. (1) Failure rates and repair time for optical components.

Module	***Failure Rate (R)***	***MTTR***
Fiber	2.12566E-07	(12),(12) hours
Regenerator	3.35521E-06	(2),(2) hours
Tx, Rx	3.35521E-06	2
Amp	(4.22508E-06), (2000FIT)	2,
Node	10.0E-6	6
Average Equipment Failure		2 hours

FIT: Average Failure rate in 10E09 hours.

Analytical calculations are based on reference data [8], [9], [10] as given in Table I. Where the values used in equation(2) as, failure rates λ_N and mean time to repair $MTTR_N$ for nodes, failure rate per kilometer λ_{Fiber} of fiber in the optical cable, mean time to repair $MTTR_S$ of spans, and the failure rate of optical amplifiers λ_{OA}. $MTTR_S$ applies to the complete span, i.e. repair times of optical amplifiers and fiber optical cables are considered equal. We have assumed that bidirectional Optical Amplifiers (OA) with a failure rate λ_{OA} are located every 50 kilometers on a span which yields an

optical amplifier spacing constant C_{OA} = 0.02 per kilometer. The failure rate of a span λ_S is therefore its length L multiplied by the sum of fiber failure rate per kilometer λ_{Fiber} and optical amplifier failure rate per kilometer, Figure 4 Shows the the difference between path and span:

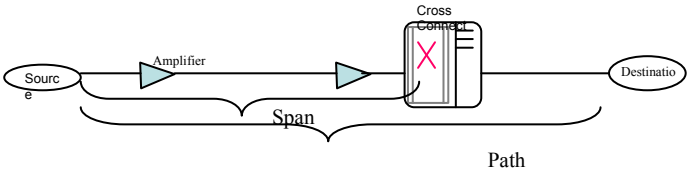

Fig. 4. End-to-end path

$$\lambda_s = L \cdot (\lambda_{Fiber} + C_{OA} \cdot \lambda_{OA}) \qquad (2)$$

A node containing the necessary line and cross connecting equipment is represented by a single block characterized by λ_N and $MTTR_N$. In order to compare the different protection strategies calculations are performed for a average span length for a long-haul networks, L_{long} = 625 km representing an average value in a long haul network, and L_{short} = 50 km, i.e. an average value in metropolitan network for comparison. In case of *no protection* the RBD of a particular connection is a simple series structure consisting of n spans and n-1 nodes with the availability expressed as:

$$A = \left(\frac{\mu_S}{\lambda_S + \mu_S}\right)^n \cdot \left(\frac{\mu_N}{\lambda_N + \mu_N}\right)^{n-1} \qquad (3)$$

Availability for generalized path protection

$$A = 2 \cdot \left(\frac{\mu_S}{\lambda_S + \mu_S}\right)^n \cdot \left(\frac{\mu_N}{\lambda_N + \mu_N}\right)^{n-1} - \left(\frac{\mu_S}{\lambda_S + \mu_S}\right)^{2n} \cdot \left(\frac{\mu_N}{\lambda_N + \mu_N}\right)^{2n-2} \qquad (4)$$

For generalized span protection

$$A = \left(1 - \frac{3\lambda_S^2}{\mu_S^2} - \frac{2\lambda_S \lambda_N}{\mu_S \mu_N}\right)^n \cdot \left(\frac{\mu_N}{\lambda_N + \mu_N}\right)^{n-1} \qquad (5)$$

We use these three equations to calculate availability in different conditions.

4. Simulation Results:

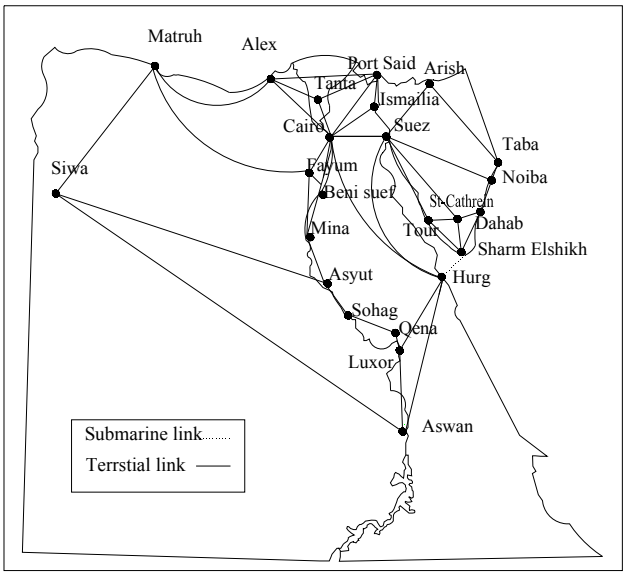

Fig. 5 Optical Transport Network.

A proposed network between the 23 biggest Egyptian cities (nodes), are shown in Fig. 5. The distance range 91 Km to 1416 Km, the distance between amplifiers is kept constant (50 Km). The data in table 1 are substituted in equations 3, 4, and 5. The unavailability of the networks is shown in Figures 6, 7, and 8 for different distances. When using 91 Km in the equations, span protection is better than path protection as shown in Figure 6. This is due to span failure rates are low, also spans have redundancy where as nodes of working path represent single point of failures in the case of span protection, this is not affected for longer spans.

For larger distances and number of nodes more than 14 nodes, the path protection is preferred than span protection because of the multiple routes available through the whole network. However span protection is performing better when the network contains a smaller number of nodes as shown in Figure 7.

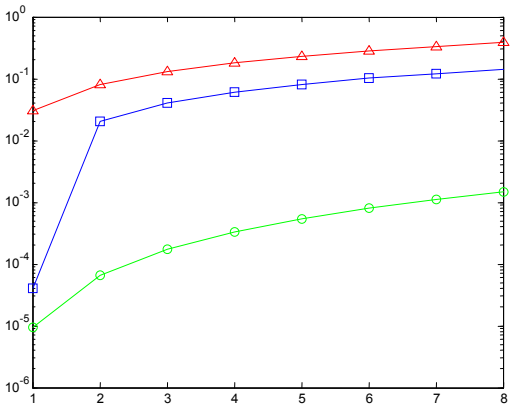

Fig.6 Unavailability for short distances 91 Km, MTTRn=6h/year

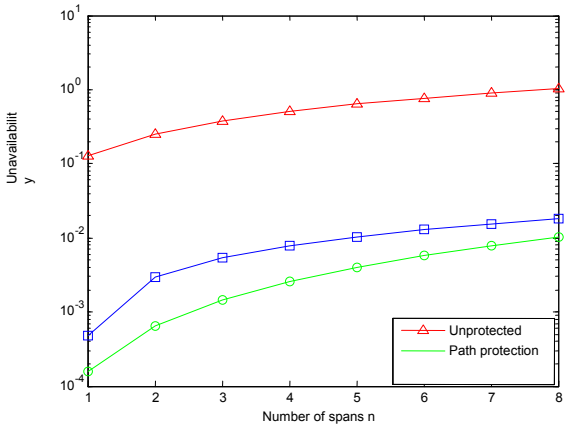

Fig.7 Unavailability for moderate distances 375 Km, MTTRn=6h/year.

For the distances in between, which the pan European network [11], suggest that the short span length will be 50 Km, and the longest span length 625 Km. The path protection perform better than the span protection till six spans, for the larger number of spans the span protection is better.

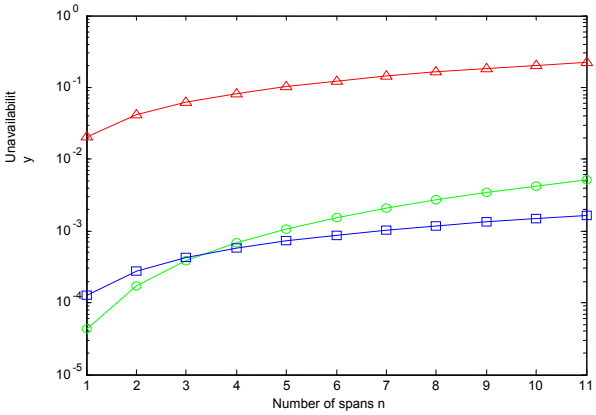

Fig. 8. Unavailability for long distances 617 Km, MTTRn=6h/year.

We can see for long distances path protection is preferred than span protection, for four spans then the span protection is better for larger numbers of spans, which requires less spans (4) to have span protection for the large distances.

Path protection is better for short spans because of the fact that span failure rates are relatively low and spans have redundancy whereas the nodes of the working represent single point of failures in the case of span protection. But for long spans span protection is better

because protection of each span makes this type of network can survive simultaneous cable breaks as long as there is not simultaneous failure for the working path and it's protection. When changing any parameter that will affect the availability of the network (i.e. MTTRn= 20 h/ year), and keeping all other parameters are constant, with the short distance 91 Km.

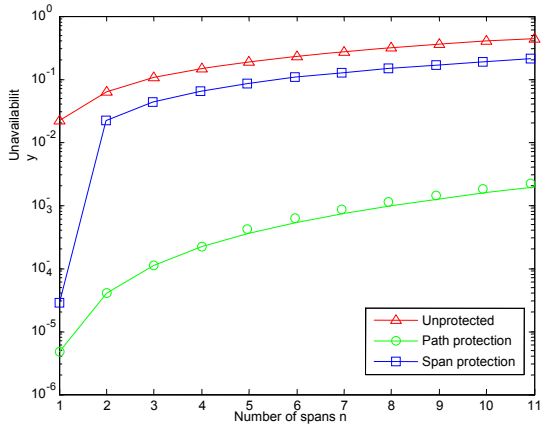

Fig. 9.Unavailability vs., no. of spans n, for distance 91km, MTTRn =20h/year

When comparing the two figures fig. 6,9. the unavailability increases for both span and path protection, but the span protection nearly reach the unprotected values, because of more components are used in the span. For the long distances the behavior will be seen in figure 9, comparing the two figures (fig. 8,10), the unavailability increases, and also the number of spans increases from 4 spans to 7 spans.

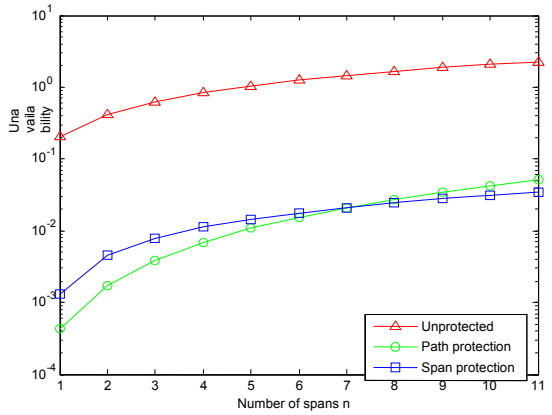

Fig. 10. Unavailability vs., no. of spans n, for distance 617, MTTRn =20h/year

CONCLUSION

The availability models for Optical Transport Networks have been presented, and a purposed network lightpaths of 23 biggest Egyptian cities is studied. The simulation results of the performance can be improved by applying the path protection or span protection according to geographic distribution of the nodes at the ends of the path. The span protection is preferred for long distances while the path protection is more efficient in short distances. And any change in the parameters like MTTRn will lead for downing the availability of the network. The algorithms used can be applied for different networks design, for both availability calculations and solution qualification.

11. REFERENCES

[1] M. Tornatore, G. Maier, A. Pattavina, "Availability Design of Optical Transport Network", IEEE J. Sel. Areas Comm.,Vol.23, NO.8, pp.1520-1532, August 2005.

[2] G. Birkin, J. Kennington, E. Olininck, A. Ortynski, and G. Spider, "Design Strategies for Meeting Unavailability Targets Using Dedicated Protection DWDM Networks ". Availableat http://engre.smu.edu/~jlk/ publications. Html.

[3] W.D. Gover, Mesh-Based Survivable Networks, Publisher: Prentice Hall PTR, August 26, 2003.

[4]Matthieu Clouqueur, Wayne D. Grover, "Availability nalysis of Span-Restorable Mesh Networks", IEEE J. Sel. Areas Comm.., Vol.20, NO.4, pp.810-821, May 2002.

[5] S. Ramamurthy, L Sahasrabuddhe, Biswanath Mukherjee, " Survivable WDM Mesh Networks", IEEE J. Light Wave Tech., Vol. 21, No.4, April 2003.

[6]Wayne D. Grover, "High availability path design in ring-based optical networks", IEEE/ACM Trans. On networks, vol. 7. No.4, August 1999.

[7]T. H. Shake., B. HazzardÁ, D. Marquis, " Assessing Network Infrastructure Vulnerabilities to Physical Layer Attacks", This work was sponsored by the

Defense Advance Research Projects Agency under Air Force Contract F19628-95-C-0002

[8] M. Held, L. Wosinska, p. M. Nellen, C. Mauz, "Consideration of connection availability optimization in optical networks", This work was partly financed by the Swiss Federal Office for Education and Science BBW (project C01.0087).

[9] M. To, and P. Neusy, "Unavailability of Long Haul Networks", IEEE J. Sel. Areas Comm., Vol.12, NO.1, pp100-110, January 1994.

[10] Hakki C. Cankaya, Ana Lardies, and Gary W. Easter, "Availability- aware Analysis and Evaluation of Mesh and Ring Architectures for long-haul Networks", Available at http://www.Scs.org/getDoc. cfm? d=1643.

[11] Wosinska L., Pedersen L., "Scalability limitations of optical networks due to reliability constraints", Proceedings of *NFOEC,* 2001.