

## SOFTWARE MEASUREMENTS FOR PROTECTION CAPACITY OPTIMISATION IN SONET

*Anagnostopoulos Ioannis, Anagnostopoulos Christos, Psoroulas Ioannis, Kouzas Georgios,  
Kotsakis Stavros, Loumos Vassileios and Kayafas Eleftherios*

Department of Electrical and Computer Engineering  
National Technical University of Athens (NTUA)  
Athens, Greece

**Abstract** – During the last years, several types of network restoration techniques have been proposed and discussed. However it was evaluated that a single restoration technique cannot cover the wide range of customer's requirements on survivability and economical spare channel assignment. This is due to the fact that each technique has its own feature and properties in terms of restoration time, flexibility, applied network elements and restoration cost. A proposed Alternative Shared Self-healing Ring Algorithm (ASSRA) is placed as substitution in a phase of an algorithm, which use an integrated self-healing technique, based in the principal of evolving more than one restoration techniques. These techniques are Route Diversity (RD), Shared Self-healing Rings (SSR) and Dynamic Self-Healing algorithms. The main scope of this paper is to examine the influence of the proposed ASSRA algorithm in the restoration cost.

Keywords: software evaluation, network survivability, integration, algorithms.

### 1. INTRODUCTION

Nowadays, developments in information technology and telecommunications have expanded drastically users as well as business communication demands for data, video and voice transmission. Large companies require high speed and volume data transmission, video teleconferencing, network management with remote control and simultaneous delivery of voice and data [2]. An optical network technology is a key factor for meeting these demands. SONET, which was formulated by the ECSA for ANSI, sets standards in the United States for telecommunications and other industries. The increased configuration flexibility and bandwidth availability of SONET provides significant advantages over older telecommunications systems.

#### *1.1. Network Elements in a SONET environment*

In this section a short description of the basic SONET Network Elements (NE) is presented and related issues are discussed.

A SONET Multiplexer (SONET mux) is a basic equipment for a SONET system. This type of multiplexer combines multiple signals into a single channel for transmission over a common facility and performs optical to electrical conversions. The SONET mux operates in two modes, the Add-Drop mode and the Terminal mode. In Add-Drop mode, a SONET ADM has direct access to the payload. It is not necessary to de-multiplex and re-multiplex the entire signal. This operation is possible as the location of each payload is specifically identified within the STS. In addition, the ADM is programmable and the user can specify which payload to add or drop from the overhead of the STS signal. Furthermore, the user can create action scenarios to handle failures by specifying where to add or drop each payload. Moreover these scenarios can be stored in a repository and initiated accordingly in case of failures. [1],[3],[4]. In terminal mode, the SONET mux acts as termination point for high-speed fiber optic signals that are de-multiplexed into slower speed constituents [3],[4]. This mode does not support add/drop capabilities.

A Digital Cross-connect System (DCS), cross connects two signals originated from different sources in a Network Element. In other words the DCS is a NE capable to terminate standard digital signals while cross-connecting constituent signals at a low speed digital signal level. Thus, before entering a DCS, fiber multiplexing systems de-multiplex signals from higher optical rates to electrical rates, requiring the use of an additional multiplexer. SONET-based DCS allow SONET optical rates to enter, be groomed inside and exit through an electrical interface [3],[4]. By exploiting the above characteristics of the DCS, at the present study the terminal mode of a SONET mux is not taken into consideration. Finally, as well as in the ADM an action scenario repository can be developed to handle failures.

### 2. SURVIVABILITY AND INTEGRATION

Taking a practical SONET environment into account, major organizations and companies have to secure the survivability of their networks. The term survivability

describes the capability of a network to restore its functions and services in acceptable levels, in case that a failure occurs. Total survivability is often not an economical choice. The most common method of providing survivability is through one or more forms of diversity. Diversity in a network is the separation or duplication of all or some of its network elements. There are several kinds of network diversities used alone or in combination, providing various levels of network survivability. In this paper, more than one protection techniques or self-healing schemes are combined to guarantee survivability in an economical spare channel [1],[5],[6]. Spare channels are the alternative way to restore the capacity of the failed working channels.

At this point, advanced algorithms are involved to integrate more than one restoration techniques. The main purpose of this integration is to optimise spare channel assignment. The proposed algorithm integrates three independent restoration techniques, namely the Route Diversity (RD), the Shared Self-healing Rings (SSR) and the Dynamic Self-Healing algorithms (DSH) [1]. Each technique has its own features and properties in terms of restoration time, flexibility, applied network elements and restoration cost as shown in Table 1. RD provides a duplicate transmission path in the form of a totally separate route. It is the fastest restoration technique but assigns a large amount of spare capacity. SSR uses a ring topology as survivability method. This kind of survivability is used in many Local Area Networks (LANs). This scheme offers certain advantages over asynchronous equipment, due to the fact that a network ring can share common facilities by using the fiber ports of a SONET mux. This type of environment facilitates add or drop signals at each network without de-multiplexing or re-multiplexing them. A ring is considered as self-healing if it can switch traffic onto a diverse protection path in case of system failure. In that scheme, the restoration is not as fast as in the previous one, but the spare capacity is much lower.

TABLE I. Features and properties of restoration techniques

	Resp. Time	Flex.	Reliab.	Share Cap.	Spare Cap.
RD	Excellent	Poor	Satisfying	Poor	Poor
SSR	Satisfying	Good	Good	Excellent	Good
DSH	Good	Good	Good	Good	Excellent

At the end, DSH algorithms restore a network, upon detection of a failure, by performing a distributed control in each intelligent network element. This technique excels in the field of spare capacity (most economical) but the network restores its services much slower than in the previous schemes. The basic network elements for the implementation of DSH algorithms are the Digital Cross connect Systems (DCS), while in the first two schemes, both DCS and Add-Drop Multiplexers (ADM) are used.

### 3. THE INTEGRATED SELF-HEALING SCHEME

#### 3.1. Overview

Rapid advances in fiber optics and VLSI technology support high-speed transport systems such as SONET. In the

case of high-speed fiber networks, failures in the transmission medium or in key fiber optic systems, like ADM or DCS can cause huge losses in bandwidth, services and finally revenue to the operating companies. Thus, a design of a Self-Healing Scheme based on the above attributes of integration is one of the most essential elements for an effectively network operation [6].

#### 3.2. Problem Definition – Results

In order to comprehend the nature of the problem, a software developer, must have the following:

##### Input:

- network's Topology (see Figure 1)
- end to end communication demands for every applied self-healing technique (see Table 2)

##### Scope:

- minimize total capacity (working + spare)

The key concept of the algorithmic procedures, as well as other inputs and issues of the problem, is briefly explained in ref. [1,] where:

$$\text{DSH d.r} = \frac{\text{DSH demands}}{(\text{DSH} + \text{SSR}) \text{ demands}} = \frac{12}{47} = 0.26$$

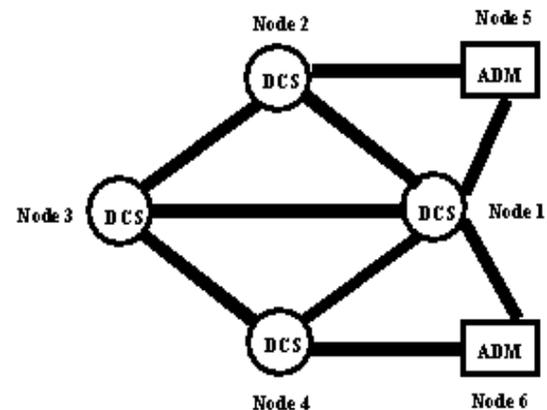


Fig. 1. Network elements and topology

TABLE II. Communication demands for DSH d.r.=0.26

	1	2	3	4	5	6
1		4 SSR 2 DSH	4 SSR 2 DSH	4 SSR 2 DSH	2 SSR	2 SSR
2			4 SSR 2 DSH	4 SSR 2 DSH	2 SSR	1 SSR
3				4 SSR 2 DSH		
4					1 SSR	2 SSR
5						1 SSR
6						

### 4. ALTERNATIVE PROPOSED SSR ALGORITHM

Considering a better way to employ more than one scheme as a survivability method for a whole network, the important issue is to share as much as possible the protection rings of the SSR restoration technique with the other protection schemes. Thus, the development of the SSR

designing algorithm must be focused in a way that will optimise the total protection capacity. However, protection ring designs may use multiple schemes, even if the nodes to node communications demands are the same. This is due to the fact that there are several algorithmic methods, which organises protection rings to satisfy normal operation of the SSR. Therefore, the key concept of this work is the comparison of two algorithmic procedures in the initial algorithm for the SSR sub-network design phase [1]. Moreover, the influence of the above algorithms on the amount of the total capacity it is examined. However, in all circumstances, the shortest path problem is taken into consideration. The outcome is that survivability is achieved even with more economical spare channel assignment.

Taking into consideration the work done by Okanou et al. in Ref. [1], the loop 3 is modified accordingly and presented in the following steps:

Let  $i$  be the indicator of the demands

$j$  be the indicator of the longest working routes

$q$  be the node set indicator of the formed rings

{/\* design the protection rings for all the communication demands \*/

- **Step 1:** initialisation
- **Step 2:** **for** (all the demands)  
    **find** the longest working routes
- **Step 3:** **for** (the  $j^{\text{th}}$  longest working route)  
    assign as protection ring, the ring that is formed from this working route and its alternative route, based in the shortest path solution.
- **Step 4:** **while** (this formed ring is enable to protect the ( $i^{\text{th}}$ ) demand) this ring is assigned as protection ring for this demand  
    **else**  $i=i+1$   
    go to **Step 3**  
    go to **Step 2**
- **Step 5:** **while** ( $q$  is sub-set of ( $q+1$ ) node set)  
    assign as protection ring that which is determined by the ( $q+1$ ) node set  
    **else**  $q$  forms the protection ring  
    **end**

Table 3 shows how the protection schemes are formed according the longest working routes as well as their respective demand capacity. Additionally in Table 4 the SSR working and spare capacity, the DSH working and spare capacity and the total amounts according to the DSH demand ratio are being deposited.

As it shown in the algorithm flow, in step 5 dominant schemes are getting involved, reducing the total number of the formed protection rings. A dominant scheme, offers its protection services to other included schemes, in the sense that it is a hyper set over a smaller one. Table 3 and Figure 2 presents the formed protection schemes for the tested case (DSH d.r.=0.26) as well as the dominant protection schemes (one in this case). In particular, four protection ring schemes are getting involved namely 2-3-4-6-1-2, 2-1-4-3-2, 4-3-2-5-1-4 and 5-2-3-4-6-1-5. However, the last scheme is the dominant one with 8 protection links in each physical link (total 48).

## 5. TOLERANCE PARAMETER (T)

In this paper a new proposed parameter is additionally considered and evaluated for the design of protection schemes. This parameter is called T (Tolerance parameter) and for an already designed network, reflects the ability to provide its services for extra communication demands. The previous paragraphs describe the influence over the total capacity of the embedded algorithm (ASSRA). This algorithm designs protection rings for specific communication demands as described above. However, it was evaluated that the designed networks can use the protection rings in order to provide extra communication demands, without losing the ability to restore their services in case of a malfunction.

TABLE III. ASSRA protection rings – dominant scheme and capacities for d.r.=0.26

Longest Working Route	Protection Schemes	Protected Working Routes (demand)
2-1-6	2-3-4-6-1-2	2-1 (1)
		1-6 (2)
		1-2 (4)
		1-3 (4)
		1-4 (4)
		1-6 (1)
		2-3 (4)
		3-4 (4)
2-3-4	2-1-4-3-2	2-3 (4)
		3-4 (4)
4-1-5	4-3-2-5-1-4	4-1 (1)
		1-5 (1)
		1-5 (2)
5-1-6	5-2-3-4-6-1-5	5-1 (1)
		1-6 (1)
Dominant Protection Scheme		Protection Capacity
5-2-3-4-6-1-5		48

TABLE IV. ASSRA d.r value and respective capacities

DSH d.r.	0.00	0.13	0.26	0.38	0.51	0.64	0.77
SSR w.cap.	56	49	42	35	28	21	14
DSH w.cap.	0	7	14	21	28	35	42
Total w.cap.	56	56	56	56	56	56	56
SSR sp.cap.	72	60	48	36	24	24	24
DSH sp.cap.	0	3	6	9	18	21	24
Total sp.cap.	72	63	54	45	42	45	48
Total cap.	128	119	110	101	98	101	104

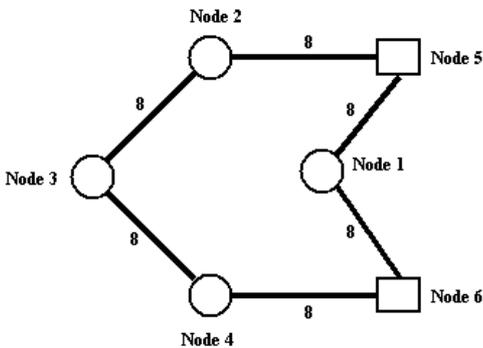
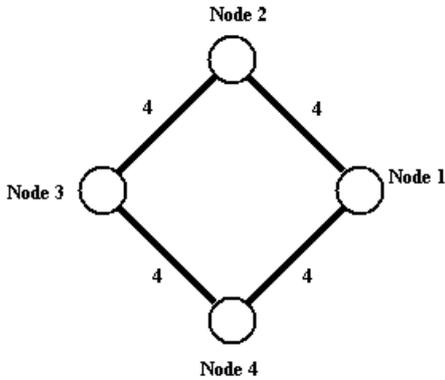
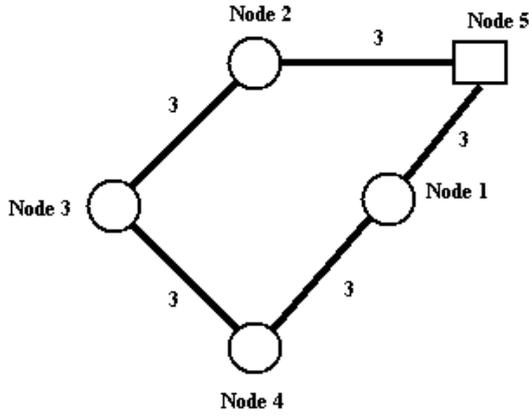
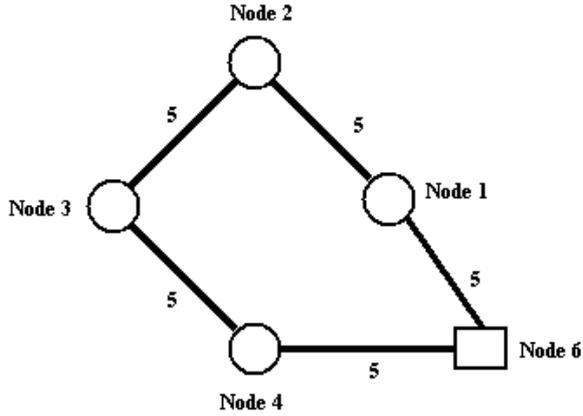


Fig. 2. ASSRA protection rings – dominant scheme and capacities for d.r.=0.26

For further evaluation, this paper proposes equation 1, which defines the network tolerance (T) in extra

communication demands for the  $i^{\text{th}}$  physical link between two network nodes.

$$T_{(i)} = S_{(i)} - W_{0(i)} \quad (1)$$

where,

$$S_{(i)} = R_1 + 2R_2 - R_3,$$

$R_1$ : the number of the SSR protection rings, which contain the  $i^{\text{th}}$  physical link,

$R_2$ : the number of the SSR protection rings, which contain the terminal nodes of the  $i^{\text{th}}$  physical link, but not the  $i^{\text{th}}$  physical link and

$R_3, W_0$ : the capacity in STS-1 of the SSR and DSH protection scheme in the  $i^{\text{th}}$  physical link respectively.

## 6. A RESTORATION EXAMPLE

This paragraph, presents an example of how ASSRA assigns protection ring schemes for the network topology of figure 1. In this example, the DSH demand ratio is equal to 0.26 and the respective communication demands for every applied self-healing technique are presented in table 2. Furthermore, table 5 holds all the above-mentioned parameters for the nine physical links of the specific network topology.

The T parameter in the last column of table 5, determines the number of SSR communication demands in STS-1, which can be additionally restored by the protection schemes. For example, the protection rings between nodes 1,2 can cover up to 7 extra communication demands accordingly to equation 1, while they cannot cover any extra communication demands between nodes 2,3 respectively. As result, in this example, ASSRA assigns an integrated protection scheme capable to restore up to 44 extra SSR communication demands. This means that even if all extra demands are involved, the same protection schemes will be assigned for protection. However, the extra communication demands will change the DSH d.r. according to equation 2.

$$\{DSH\ d.r.\}_n = \left(\frac{T_0}{T_0 + T}\right) * \{DSH\ d.r.\}_i \quad (2)$$

Table 6 now holds the communication demands for the new defined ratio. In the described example the new value of the DSH d.r. is equal to 0.13, while the total capacity remains 110 in STS-1. Finally, table 7 depicts the nDSH d.r., according DSH d.r. and Tolerance parameter (T).

TABLE V. Applied network parameters

Origin Node	Terminal Node	R1	R2	R3	Wo	S	W	T
1	2	0	8	5	4	11	0	7
1	3	0	8	4	2	12	0	10
1	4	0	8	5	4	11	0	7
1	5	8	0	4	0	4	0	4
1	6	8	0	4	0	4	0	4
2	3	8	0	8	2	0	2	0
2	5	8	0	2	0	6	0	6
3	4	8	0	8	2	0	2	0
4	6	8	0	2	0	6	0	6

TABLE VI. Communication demands for  $\{DSH\ d.r.\}_n=0.13$

	1	2	3	4	5	6
1		12 SSR 2 DSH	24 SSR 2 DSH	14 SSR 2 DSH	2 SSR	4 SSR
2			7 SSR 2 DSH	4 SSR 2 DSH	4 SSR	1 SSR
3				7 SSR 2 DSH		
4					1 SSR	6 SSR
5						1 SSR
6						

TABLE VII. Tolerance and DSH d.r. values for ASSRA

DSH d. r.	Tolerance	nDSH d.r.
0	88	0
0,13	66	0,05
0,26	44	0,13
0,38	22	0,26
0,51	6	0,45
0,64	7	0,56
0,77	8	0,66

## 7. CONCLUSIONS

In section 4, the measurements and the topology taken under consideration are described as complement to ref [1]. The scope is to facilitate comparison between the inputs and results of the actual work done in the previously referenced work.

Furthermore, additional measurements for all the DSH demand ratios over the total capacity had been taken. In this way, the influence of ASSRA algorithm is shown in Fig. 3. Table 4 depicts the total capacity (working + protection) for ASSRA algorithm in respect to the protective demand ratio. It must be noticed that the total capacity for ASSRA is the result of the modification proposed over the sub-network design phase (loop 3), of the integrated self-healing algorithm (OSH) suggested by Okanou et al.

As result, it is proved that, without violating the protective demand ratio, different algorithmic procedures in the design of the protection rings lead in different results. Furthermore, the benefits of an integrated self-healing technique are verified clearly in the case of spare channel assignment. This is due to the fact that, for the implemented algorithm, when DSH d.r. is increased, the total capacity of the network is decreased. This is particularly obvious in the area where different schemes act simultaneously and at the same grade to provide protection (DSH d.r. close to 0.5).

From the comparison between the two proposed protection ring algorithms, it is concluded that if these dedicated rings share the protection, DSH scheme is employed in a larger scale, providing a better integration of these self-healing techniques. ASSRA supports this feature in an efficient way, through the dominant protection rings as

it is reflected in figure 3.

However, ASSRA fails to design in a more economical way the tested network for demand ratio lower than 0.26 (point A). Nevertheless, the use of the T parameter in the designing procedure, decrease this value. In Figure 4, a slightly shift to the left is occurred for every value set of the total capacity and nDSH d.r., as described analytically in equation 2 and tables 5,6,7. As result, when T parameter is taken under consideration, ASSRA designs the tested network in a more economical way, when the d.r ratio exceeds the value of 0.08 respectively (point B).

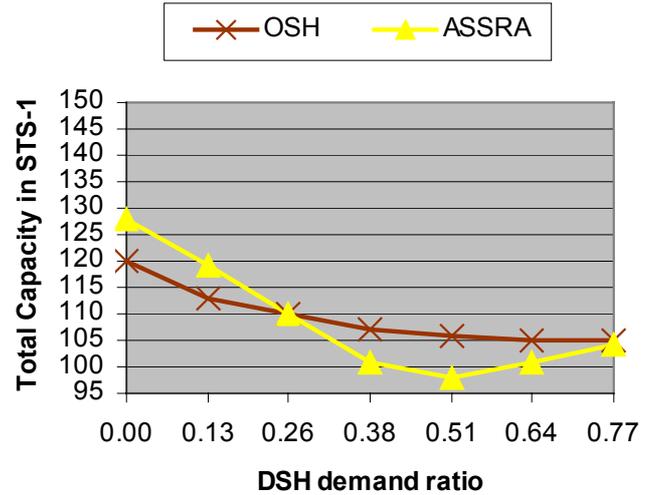


Fig. 3. Total capacities over different DSH d.r.

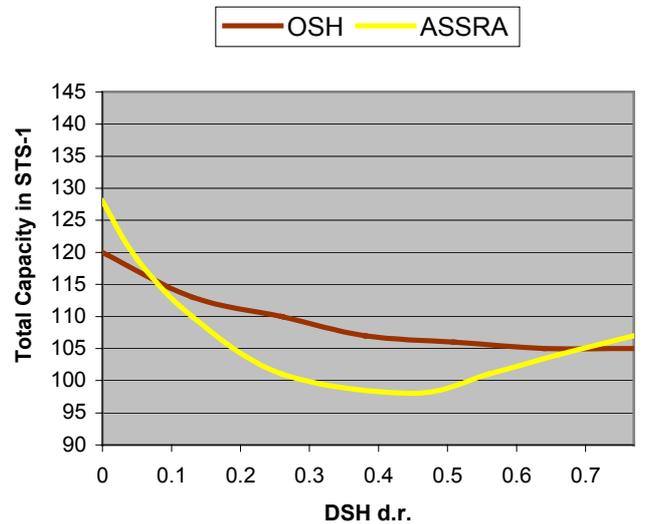


Fig. 3. Total capacity optimisation

Figure 4 presents the total capacity of the designed network in STS-1 according to their respective demand ratios, when the proposed T parameter is considered in the whole algorithmic procedure of ASSRA. Values, which vary between points B and C, highlight the areas where ASSRA has an advantage in the amount of the total capacity, compared to the results of the initial proposed algorithm by Okanou et al. in ref. [1]. Thus, this paper proposes ASSRA

enforced with T parameter, as described in sections 4, 5 and 6, as an efficient algorithm for capacity optimisation in protection schemes for optical networks.

#### REFERENCES

- [1] Yasuyo Okanoue, Hideki Sakauchi and Satoshi Hasegawa, 'Design and Control Issues of Integrated Self-Healing Networks in SONET', *IEEE Globecom91* (1991)
- [2] Data and Computer Communications, W.Stallings, Macmillan, 1999
- [3] Advances in Transport Network Technologies: Photonic Networks, ATM, and SDH, KEN-ICHI SATO, Artech House Telecommunications Library, 1997
- [4] Transmission Networking: SONET and the Synchronous Digital Hierarchy, Mike Sexton, Andy Reid, Artech House, 1992
- [5] Hideki Sakauchi, Yasuyo Nishimura and Satoshi Hasegawa, 'A Self-Healing Network with an Economical Spare-Channel Assignment', *IEEE Globecom90* (1990)
- [6] C. Han Yang and Satoshi Hasegawa, 'FITNESS: Failure Immunization Technology for Network Service Survivability', *IEEE Globecom88* (1988)

---

Mr. Anagnostopoulos Ioannis  
Dr. Anagnostopoulos Christos  
Mr. Psoroulas Ioannis  
Mr. Kouzas Georgios  
Mr. Kotsakis Stavros  
Prof. Loumos Vassileios  
Prof. Kayafas Eleftherios

Department of Electrical and Computer Engineering, National Technical University of Athens (NTUA)  
9, Heroon Polytechniou Str., Zographou, Athens, Greece  
Tel: +30 1 772 2538, Fax: +30 1 772 2538  
Contact author e-mail address: [janag@telecom.ece.ntua.gr](mailto:janag@telecom.ece.ntua.gr)

---