Network Protocols and Algorithms
ISSN 1943-3581
2009, Vol. 1, No. 1

Compound OD Cycles for a Wide Variety of Survivability Policies in Transport Networks

Meir Herzberg
ECI Telecom, Network Solutions Division,
30 Hasivim Street, Petach-Tikva 49517, Israel
E-mail: Meir.Herzberg@ecitele.com

Felix Shleifer
ECI Telecom, Network Solutions Division,
30 Hasivim Street, Petach-Tikva 49517, Israel
E-mail: Felix.Shleifer@ecitele.com

Regina Ring
ECI Telecom, Network Solutions Division,
30 Hasivim Street, Petach-Tikva 49517, Israel
E-mail: Regina.Ring@ecitele.com

Abstract

Converged telecommunication networks, which simultaneously support a growing variety of services through a common network infrastructure, are aimed at significantly reducing network expenditures. This trend has encouraged the development of a unified network paradigm capable of supporting a wide variety of cost-effective recovery solutions, each of which may cope differently with fiber cuts and nodal equipment failures in order to satisfy service-dependent requirements. Expansion of the Origin-Destination (OD) Cycles approach is used to meet that challenge by offering ten different policies for survivability and their relative performance measures in terms of consumption of network resources and the resulting times of recovery. For practical purposes the scope of failure scenarios is limited to single and double-network failures only, even though the approach suggested is generic and can basically address even more complex events. Three test networks are extensively analyzed to demonstrate the paradigm developed and to present some useful observations about the relative positioning of the policies considered for survivability

Key Words: Converged Networks, Network Survivability, OD Cycles, Integer-linear Programming

1. Introduction

We adopt in this paper a carrier's viewpoint, relying on complete knowledge of a given fiber-optic infrastructure, including internal details such as Shared Risk Link Group (SRLG) and transport network equipment capabilities at the network nodes, to support a given set of telecommunication services. Based on this information, the purpose is to present a unified network paradigm through which carriers may offer and charge customers for using suitable recovery schemes in the event of transport network failures such as fiber cuts or nodal equipment malfunctions. The motivation for allowing a wide-range of recovery solutions stems from the general trend for the creation of converged networks that support the growing number of services through a common and costly network infrastructure aimed at reducing significantly both Capital and Operational Expenditures (CAPEX and OPEX). The growth in the number of services and applications in the IP network environment today has yielded, for example, the shift from the Integrated Services (IntServ) reference to the more adaptive Differentiated Services (DiffServ) model [2]. Such a refinement naturally inspires network-survivability differentiations as well, e.g. [18].

Major challenges of network survivability to meet the above developments are:

- Selecting a generic network approach that encompasses a broad range of service-dependent survivability policies;
- Developing a practical-oriented network model and embedding network algorithms to support a wide-variety of survivability policies;
- Obtaining high-quality model results by taking into account common and costly network resources for any possible subset of survivability policies considered.

We limit the scope of failure scenarios to single and double-network failures, referring both to link, node and SRLG network failures. The two reasons for this are purely economic: (i) Based on [20] the probability of triple simultaneous-network failures in developed countries is low and policies for such cases are expected to be quite demanding in terms of overall network resources; (ii) Based on the experience gained by analyzing numerous real-transport networks worldwide, most networks face physical limitations associated with low Average Nodal Degrees (AvND), usually less than four, which technically cannot guarantee coping with triple failures. Despite that, it is still possible to handle to a limited extent more than two simultaneous failures, see for example Figure 2(b).

Strategies for network survivability [25] vary considerably. We restrict the state space of network survivability to three major dimensions: (i) Scope of recovery to bypass failure impact, taking into account the main recovery alternatives of link/span/node (element), Failure-Independent and Failure-Dependent end-to-end Path (FIP) and (FDP); (ii) Nature of backup resources, selecting the options of Dedicated (DE), Shared (SH) or Dedicated Split (DSP) which meets traffic demands by using multi paths; (iii) Trail setup mode due to failures, choosing the two polar alternatives of either Proactive (PRA), where backup paths and resources along these paths are prepared in advance, prior to failure, or Reactive (REA), where end-to-end backup trails are established following failures. For simplicity, we overlook some complementary factors such as: mode of network surveillance (centralized or distributed), which is correlated with the nature of backup resources and trail setup mode; multi-layer survivability, usually oriented to specific network technologies, and multi-domain networks that considers heterogeneous areas. We also overlook the phase of path calculation (pre- or post-fault calculations for recovery route selection), focusing only on end results of trail setup that covers both path selection and actual assignment of resources along the paths.

A combined selection from dimensions (i)-(iii) once (twice) to cope with any single (double) failures, determines a policy for survivability. Selecting the combination of FIP-DE-PRA for any single failure, for instance, represents the traditional 1+1 path-protection policy, usually implemented through Automatic Protection Switching (APS) at path termination points. Using the FIP-DE-PRA combination twice, for two consecutive failures, represents the Triple Way Protection (TWP) or simply 1+1+1 path-protection policy. For practical purposes we restrict double-network failure policies as follows: A policy that selects different combinations of dimensions (i)-(iii) can be accepted only if the resulting recovery times from the first failures are expected to be *no longer* than the recovery times from the second failures. Such a restriction tends to favor first failures, aimed at restraining network escalation. We relate the "first" and "second" (or "next") failure with reference to the home position under no failure conditions. More specifically, the first failure is considered as occurring in a network that previously had not been under failure conditions while the second failure is assumed to occur in a network that previously had already been affected by the first failure.

The survivability policies discussed are basically generic and technology independent, yet adaptive to the various transport technologies, including: SONET/SDH, Asynchronous Transfer Mode, Wavelength Division Multiplexing (WDM), Optical Transport Networks (OTN) which combines benefits of both SONE/SDH and WDM, Multi-Protocol Label Switching (MPLS) and General MPLS. For example, assignment of end-to-end DSP resources may rely on either Virtual Concatenation combined with Link Capacity Adjustment Scheme, when using the SONET/SDH technologies, or on Link Aggregation (LA) together with a suitable LA Control Protocol in OTN. Traffic values associated with network load and modeling may be assigned different unit rates such as: sub-lambda rates, derived from rate hierarchy of the SONET/SDH standards; non-standard high rates, derived from the Generic Framing Procedure that provides an adaptive mechanism for agnostic frames; wavelength units in WDM networks for photonic recovery at typical rates of 2.5, 10 and 40 Gbps; or simply explicit data-rate units in terms of Mbps, when applicable.

Previous work:

There are a large number of publications in the area of network survivability. However, in the most parts they address specific issues associated with technologies and services, and usually focus on a specific policy for survivability. Reference [4] details an extensive survey on contributions made, their classification and the resulting differences on network recovery. The reference section here is limited to algorithms and perceptions that have addressed multiple-recovery aspects, including differentiated protection, multi-network services and multi failures. Reference [7] has specified the term Quality of Protection (QoP), introduced as a parallel notion to the well-known perception of Quality of Service (QoS). The p-Cycles approach, which uses shared backup resources in a proactive trail setup mode for line restoration [10], has been extended into several directions: Multi-service survivable networks using line protection and restoration are detailed in [3, 9]; work on path-protection p-Cycles has also been published [16]; expanding p-Cycles to Multi-Domain and Multi-Service Networks (MDMSNs) can be seen in [6, 23]. Various issues of Shared Backup Path Protection (SBPP) that refer to multi-recovery considerations are indicated for the following: multiple-network failures [15]; dual-link failures in WDM under differentiated Service Level Agreements (SLAs) in [11] and for recovery from double-network fault in [24]. Protection from single and double failures that evaluates performance aspects in MPLS networks is detailed in [22]. Optical network survivability with single and multiple service classes is studied in [24]. Optimal network models based on Origin-Destination (OD) Cycles to cope with three survivability policies for single-network failures have been developed [13]. Applying OD Cycles to MDMSNs has also been published [14]. References [1, 8] are useful to accomplish efficient search of disjoint OD paths, highly important in large networks. To the best of our knowledge no previous work has addressed a wide variety of survivability policies.

The rest of the paper is organized as follows: Section II explains the OD Cycles approach and the expanding directions used; Section III details the various policies for survivability that can be derived by compound OD Cycles; Section IV is dedicated to network modeling for the optimal assignment of network resources for the possible use of the considered policies; finally, Section V details numerical results following the analysis of three test networks.

2. Expending OD Cycles to Multi-network Failures

The OD Cycles approach has originally been developed to cope with single-network failures. In order to encompass more complex failure scenarios, some adaptations are needed.

2.1. Failure-Independent (FI) OD Cycles

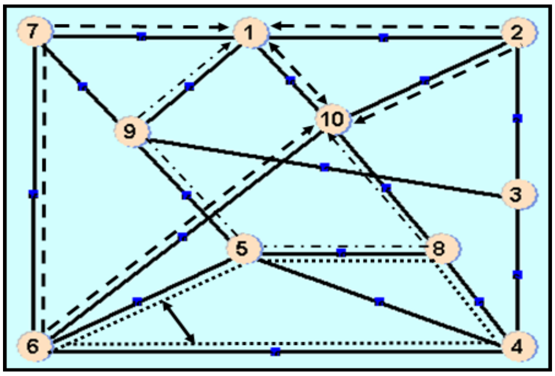


Figure 1 – An example of FI OD Cycles with different k-disjoint paths

We first refer to single-failure OD Cycles. Assume that OD pair (6-8) in Figure 1 is associated with survivable traffic. The cycle 6-5-8-4-6 (indicated by dotted lines) is composed of two paths 6-5-8 and 6-4-8. If fibers 5-6 and 4-6 traverse a common conduit or duct (indicated by a bidirectional arrow) that cycle is not eligible for OD pair (6-8) as it does not meet SRLG route-diversity considerations. Despite this, the cycle is still eligible for other OD pairs with survivable traffic, such as OD pair (4-8), composed of the 2-disjoint paths 4-8 and 4-6-5-8.

Assignment of resources to Eligible 2-Disjoint OD Paths (E2-DODPs) allows coping with single-network failures independently of failure type and location along the two disjoint paths. We use the term of FI OD Cycles to reflect that situation.

In order to cope with double failures, OD Cycles use sets of Eligible 3-Disjoint OD Paths (E3-DODPs). Figure 1 presents one set of E3-DODPs for pair (1-10), namely: 1-10, 1-2-10 and 1-7-6-10 (indicated by arrowed-dashed lines). The specific pair (1-10) can even cope with triple failures by using E4-DODP sets. One such a set can be established by including the path 1-9-5-8-10 (indicated by dot-dash lines). Clearly, not all OD pairs in this network example can cope with triple failures as the AvND = 3.6 < 4.0 (18 fibers, 10 nodes).

Choosing three out of the four disjoint paths already indicated yields for the particular pair (1-10) four different E3-DODP sets. Using another fourth path, e.g., 1-9-5-4-8-10 enlarges the different E3-DODP sets from four to eight. The reader might be surprised to know that the pair (1-10), in the network (ignoring fiber duct considerations), is associated with a total of 62 E3-DODP sets compared to 132 E2-DODP sets. The network model, based on OD Cycles, uses different E2-DODP and E3-DODP sets and only a fraction of the total sets is considered for network optimization. This can practically be done by applying some predefined filtering rules to select the most attractive OD sets. As indicated, we use references [1, 8] to find the sets E2-DODP and E3-DODP, subject to route diversity levels. For example, searching for disjoint node sets (intermediate nodes are not allowed) is more demanding than disjoint fiber sets.

We can summarize the above as follows: The use of FI OD Cycles to cope with single and double network failures results in each OD pair with survivable traffic having predetermined E2-DODP and E3-DODP sets, respectively. Quantity of sets subject to survivability policies and the resulting solution qualities are an issue of investigation in this paper.

2.2. Failure-Dependent (FD) OD Cycles

OD Cycles have also been extended to FD cases in order to cope differently with multi network failures. The motivation for this is now explained.

There is a fundamental difference between recovery considerations for single and multi failures, relying on the assumption that the inter-failure time in transport networks is in the order of hours, e.g., [20] Table 11.1. As a consequence, the probability of experiencing two consecutive independent failures within intervals of single seconds is low and can practically be neglected. Based on the above, one can assume that a proactive trail setup mode, that uses shared redundant resources after the first failure and towards the next failure, is likely to have a superfluous period towards the occurrence of the next failure. The 'privilege' of using shared backup resources towards the next failure, with almost no effect on the expected recovery times, opens new possibilities to cope with multi failures and the development of advanced cost-effective policies for survivability. If the assumption of inter-failure time does not hold or there are two simultaneous failures then for the second failure the combination FDP-SH-REA holds and recovery times from the second failure are expected to be significantly longer.

Using the FIP-DE-PRA combination for the first failure and the FDP-SH-PRA combination for the next failure has been found suitable by the Automatic Switched Optical Network (ASON) standard, e.g., [17], so as to supply rapid recoveries from multi failures. Expansion of OD Cycles to cope with such scenarios is illustrated in Figure 2.

Assume that OD pair (1-11) is assigned ASON survivable traffic for any double failures. Figure 2(a) presents Main and Protection E2-DODPs for that pair, based on the Open Shortest Path First scheme, using dashed and dotted lines, respectively, to cope rapidly with the first failure. In order to consider double failures in the FD mode, one has to address recovery from any possible first failure along the E2-DODPs, namely, possible of either node failures 2, 10, 3 and 6 (termination nodes are excluded) and fiber cuts 1-2, 2-10, 10-11, 1-3, 3-6 and 6-11.

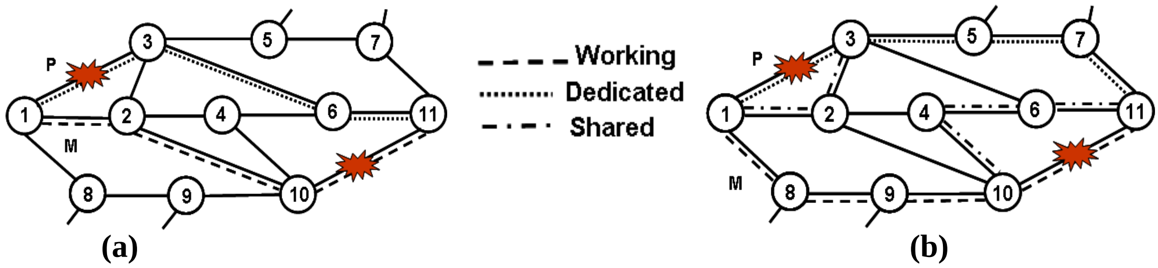


Figure 2 – Applying FD OD Cycles to ASON traffic

Consider fiber cut 10-11 (or 1-3) in Figure 2(a) being part of the working (protection) path. It can be ascertained that a recovery path from that failure, which is totally disjoint from the protection (working) path, does not exist. Such situations are known as "traps", often associated with non-disjoint path flows (see for example [5]). OD Cycles is applied to avoid trap situations by using E3-DODP sets, where the first and second paths are used for working and dedicated protection, respectively, as illustrated in Figure 2(b). The trap situation is avoided by ensuring a third disjoint path for each OD pair, only as a "hidden" safeguard for FD recoveries (in our case the horizontal path 1-2-4-6-11). The FD recovery paths following fiber cuts 1-3 and 10-11 are 1-2-3-5-7-11 and 1-8-9-10-4-6-11, respectively. Figure 2(b) also presents selective triple-failure survivability (two consecutive fiber cuts 10-11 and 1-3).

2.3. Principles and Inherent Advantages of OD Cycles

We now specify main characteristics of OD Cycles for network modeling and their expected impact on solution qualities:

1. Recovery is path based, for both FI and FD cases, where each path is associated with a specific end-to-end OD pair.

2. For each OD pair with survivable traffic, predetermined Ek-DODP sets (k=2 or k=3) are prepared, subject to the survivability policies. Having a complete knowledge of the network, only eligible sets are selected, using path lengths, path hops and SRLG considerations. Filtering of non Ek-DODP sets is done in advance, leaving the actual selection of OD path sets and their flows as a compound combinatorial problem to be solved by network optimization.

3. Each Ek-DODP set is composed of k designated paths, each two of which present an eligible OD cycle. Designated paths may function under different modes to support the variety of policies considered. The OD Cycles approach is therefore fundamentally different from the p-Cycles approach. Predetermined Ek-DODP sets are OD oriented and designated to use both working and backup resources, while predetermined protection cycles are associated with backup resources only and basically are not OD oriented.

4. FI OD Cycles gain path-based benefits (failure type and localization are not required for recovery purposes) while FD OD Cycles are more adaptive to failures.

Based on the above four principles ("P1"-"P4"), and subject to a suitable network model, one can expect to achieve high-quality results in terms of overall utilization of common network resources. This stems from the cumulative of several major advantages, as follow:

- End-to-end path-based recovery is used rather than link-based recovery, avoiding excessively long or loop-contained backup paths for recovery processes, based on "P1" or briefly ("P1").

- All types of network failures can be considered, including node, link and multi-links ("P2").

- Most attractive and numerous potential Ek-DODP sets may be included (up to any conceivable extent, e.g., all sets below predetermined OD path hop limits) as an input to the optimization process, having essentially no effect on the number of model constraints ("P2") for most policies. The last point is further discussed in Section IV.

- Working and backup OD paths are selected jointly ("P3") rather than separately, where main paths are first determined followed by backup path selection. Using a single-phase approach has clearly the potential of achieving improved results.

- A wide set of policies can be encapsulated into a single network model that uses common network resources ("P3") to satisfy all policies considered, rather than using different models to satisfy single or a small subset of policies.

- Suitable LP and ILP network models may supply lower bounds, optimal or near-optimal results through a single-computational process, including: (i) individual Ek-DODP sets selected; (ii) assignment of working and backup resources (dedicated and shared) to designated paths, subject to each policy; and (iii) the derived common network resources that support the policies considered ("P1"-"P4").

3. Survivability Policies Supported by OD Cycles

We now specify the policies for survivability that can be supported by OD Cycles. Each policy is defined by:

- A unique serial number (presented in the network model)

- A name and abbreviation for convenient purposes

- The combined selection from strategy-survivability dimensions (i)-(iii)

- Typical expected characteristics.

Policies 1-3 are used to cope with single failures and OD Cycles rely on E2-DODP sets.

1. Traditional Path Protection or briefly 1+1 with APS

Recovery uses the FIP-DE-PRA combination. The first and second OD paths within each set are designated to be working and protection paths, respectively. This is the widely-accepted policy in most telecommunication networks. Recovery times through APS are usually very short, in the order of tens of milliseconds.

2. Shared Backup with Path Protection (SBPP) or FI 1+R

Recovery relies on the FIP-SH-REA combination. The first (second) OD paths within the sets is designated to be the working (restoration) path. Despite adopting a reactive setup mode, the SBPP policy predetermines recovery paths, prior to failure events. As a result, recovery times are reduced as search for backup paths is saved. Actual recovery times are both protocol and failure dependent. The number of affected connections plays a major role on recovery times. Some applications associated with this policy may require that end-to-end traffic be assigned to a single recovery path while others may allow multi-recovery paths. The requirement of using single-recovery paths is more demanding compared to the alternative, often known as the issue of bifurcation flows. It is essential to return to the home position after fixing the failure.

3. Split Traffic or 1/2 +1/2

The combined selection of FIP-DSP-PRA is applied to this policy. No redundancy resources are actually used and the two paths within each set are designated to carry working resources. A suitable adaptation/aggregation scheme is required for implementation. The transmitter part of each connection has, for example, to be notified about the mode of working (normal, fault). Any single failure does not affect more the 50% of end-to-end traffic. For some OD pairs multi-split flows may occur and the portion of traffic affected by certain failures may be even less than 50%. Flow limits per path may encourage multi-split flows.

Policies 4-10 are aimed at coping with double failures, relying on E3-DODP sets.

4. Triple Way Protection (TWP) or 1+1+1

Recovery processes from first and second failure rely on the FIP-DE-PRA combination. The first path within each set is designated for working while the other two are designated to be the first and second protection paths. Recovery times from both first and second failures are similar to the 1+1 protection. This is a highly demanding policy that might be quite expensive. Top priority and time-critical services may use that policy, e.g., telemedicine services. Return to the home position after fixing a failure is optional.

5. Triple Way Split (TWS) or 1/3 + 1/3 + 1/3

TWS refines Split Traffic (Policy 3), relying on the FIP-DSP-PRA combinations for both first and second failures. Under normal conditions, all three paths of selected sets carry working flows. First and second failures cannot affect more than 33% and 66% of OD traffic, respectively. Such a policy may suit certain data services that can still function under different traffic rates. A suitable adaptation/aggregation scheme is required for implementation as for Policy 3.

6. Split+ or 1/2 + 1/2 + (1/2):2

This policy relies on the FIP-DSP-PRA combinations for first and second failure. Unlike the Split Traffic and TWS, this policy combines both split and redundant resources. Under normal network conditions, any OD pair is assigned the full rate traffic end to end through the first two designated working paths, leaving the third designated path as a "hot" standby to backup each one of the first two working paths. Following any single and double failures 100% and at least 50% of the original traffic, respectively, is still maintained.

7. FI Dual Shared or FI 1+R+R

This policy consumes shared backup resources only. Full recovery from the first and second failures relies on the FIP-SH-REA combination. Consumption of resources is expecting to be low and times of recovery may be relatively slow for both first and second failures as in Policy 2. The use of a network-control plan may significantly accelerate recovery times. Return to the home position is required to release the shared network resources.

8. FI P1R2 or FI 1+1+R

This policy uses different recovery arrangements. First and second failures rely on the combinations FIP-DE-PRA and FIP-SH-REA, respectively. Recovery times form first (second) failure is as in Policy 1 (Policy 2). In the event that the first failure is fixed before the second failure, recovery actions are saved and the return to the home position is optional.

9. FI P1R2 or FI 1+1+R**

Recovery from the first failure relies on the FIP-DE-PRA combination, as before, while recovery from the second failure relies on the FIP-SH-PRA combination. The first two paths within each set are used for working and dedicated protection while the third disjoint path is assigned shared resources in a proactive setup mode immediately after the occurrence of the first failure. It relies on the assumption that the inter-failure times is in the order of many minutes (see also Sec. 2.2). Rapid recovery times from first and second failures are expected. The 'star' of the term FI P1R2* is aimed at differentiating from Policy 8, reflecting the proactive mode of setup trails towards second failures, still leaving the common part P1R2 unchanged. Recovery times from second failures might be prolonged if second failures occur immediately after first failures.

10. FD P1R2 or FD 1+1+R**

This policy is similar to Policy 9 in terms of fast recovery times. The difference relates to the FD mode of recovery towards the second failure. Recovery from the first (second) failure relies on the FIP-DE-PRA (FDP-SH-PRA) combination. FD recovery paths have not been considered by all previous policies. Implementation procedures here usually rely on a control network plane with signaling capabilities to speed up recovery processes. Return to the home position is required only after the second failure. FD recovery can basically be applied in other combinations, thus increasing even further the number of possible recovery policies.

4. Network Modeling Based on OD Cycles

In this section we detail a compound network model that refers to all survivability policies discussed. The following notation is used.

Model Sets and Parameters:

N — Number of transport-network nodes, modeling index $n=1,2...,N$.

L — Number of network fibers and links, indexed $i=12,,..,L$.

V — Number of policies for survivability considered, indexed $v=1,2,..,V=10$. Each value "v" represents a specific policy, based on the serial numbers appearing in Section III.

G — Number of failure scenarios considered, including single-link, multi-link (duct) and node failures. Without loss of generality, we use the index $g=1,2,..,L$ for link failures, $g=L+1,L+2,..,L+N$ for node failures and $g=L+N+1,..,G$ for multi-link failures derived from SRLG considerations. Clearly:

$$g = \begin{cases} i, & 1 \le i \le L \\ L+n, & 1 \le n \le N \end{cases} \quad \text{for link "}i\text{" and node "}n\text{" failures} \tag{1}$$

For each compound failure $g>L$ (node and multi-link), it is required to keep the set of links being affected by the failure g.

J — Number of OD pairs associated with survivable traffic, indexed $j=1,..,J \le N*(N-1)/2$. The values $j=1,..,J$ are intentionally *policy independent*. The relationship between survivable traffic, OD pair and the related policies is clarified next by the traffic terms.

T_{jv} — Survivable traffic related to index pair "jv", $T_{jv} \ge 0$. $T_{jv} = 0$ is assigned to all cases where OD pair "j" is not associated with the policy "v", $j=1,2,..,J$, $v=1,2,..,V$. In this way we can accommodate any subset of survivability policies.

We assume that survivable traffic is bidirectional. This assumption is valid for most network services. The use of unidirectional traffic, e.g., broadcasting, requires some model adaptations such as: (i) the value J may even be doubled, (ii) link directions along OD paths within each Ek-DODP set should be taken into considerations; (iii) separate bookkeeping of resource assignment on each two-link directions is actually required. Another hidden assumption is related to traffic units. It is quite possible that different traffic units are associated with the index pair "jv", using actually a vector of traffic values, each of which represents a certain traffic unit.

For such cases, separate bookkeeping should be done for each unit. Traffic unit weights should be considered to calculate properly total network link resources and loads.

λ_{jv} Modeling traffic value associated with index pair "*jv*". Modeling values are different from traffic values only for policies that use split traffic, specifically:

$$\lambda_{jv} = \begin{cases} T_{jv} & 1 \le v \le 10 \quad v \ne 3,5,6 \\ \lceil T_{jv}/2 \rceil & v = 3 \\ \lceil T_{jv}/3 \rceil & v = 5,6 \end{cases} \tag{2}$$

$R_j(k)$ Number of Ek-DODP sets related to pair "*j*", indexed $r=1,2,.., R_j(k)$, $j=1,..,J$. For Policies 1-3 (4-10) the value *k=2 (k=3)* is used. Clearly, triple network failure policies require using *k=4*. For Policy 10 the value *k=1* is used to select for each OD pair *"j"* the most $R_j(1)$ attractive paths with no route-diversity restrictions.

$R_j^g(1)$ Number of eligible FD recovery paths related to pair "*j*" due to failure "*g*", indexed $q=1,2,..., R_j^g(1)$, $j=1,2,..,J;\ g=1,2,.,G$. Eligible $R_j^g(1)$ paths can practically be derived from $R_j(1)$ by excluding paths that cannot be considered for recovery due to failure "*g*".

$\delta_{jr}^i(pk)$ A binary coefficient, gets the value "1" if the p*th* path associated with the r*th* Ek-DODP set, associated with OD pair "*j*", passes through link "*i*" and "0" otherwise; $i=1,2,..,L;\ j=1,..,J;\ r=1,.., R_j(k);\ k=1,2,3;\ 1 \le p \le k$. We use the terms $\delta_{jr}^g(pk)$ to address link failures, *g≤L*. For such cases we define $\delta_{jr}^g(pk) \equiv 0$ if *g>L*. For the special case *p=k=1*, the binary coefficients are also applied, using the paths $R_j^g(1)$ for which $\delta_{jq}^i(1,1)$ gets the value "1" if the path "*q*" associated with OD pair "*j*" passes through link "*i*" and "0" otherwise; $j=1,2,..,J;\ i=1,2,..,L;\ q=1,2,.., R_j^g(1);\ g=1,2,..,G$.

$\varepsilon_{jr}^n(pk)$ A binary coefficient, gets the value "1" if the *p*th path associated with the ***r**th*, Ek-DODP set, associated with OD pair "*j*", passes through node "*n*" and "0" otherwise; $n=1,2,..,N;\ j=1,..,J;\ r=1,.., R_j(k);\ k=1,2,3;\ 1 \le p \le k$. We use the terms $\varepsilon_{jr}^{g-L}(pk)$ to address node failures, *g>L*. For such cases we define $\varepsilon_{jr}^{g-L}(pk) \equiv 0$ if *g≤L*. For the special case *p=k=1*, the binary coefficients are also applied, using the paths $R_j^g(1)$ for which $\varepsilon_{jq}^{g-L}(1,1)$ gets the value "1" if the path "*q*" associated with OD pair "*j*" passes through node "*n*" and "0" otherwise; $j=1,2,..,J;\ n=1,2,..,N;\ q=1,2,.., R_j^g(1);\ g>L$.

M Single modularity value, represents the amount of traffic that can be accommodated within a single transmission system. For different traffic units, *M* is calculated based on the common denominator used for all traffic unites. It is possible to consider multi-modular values, which are to a large extent equipment-vendor dependent.

C_i Cost of each transmission system assigned to link "i". In networks where links distances are quite similar, e.g., Metropolitan Area Networks, the cost per transmission system can be constant and link independent.

U An upper percentile of resource utilization level, 0<U≤100. This predetermined parameter considers planning aspects not within the scope of the model, such as: unprotected traffic, regulation guidelines and future-growth margins.

Model Variables:

X_i Number of common transport systems assigned to link i, $i=1,2,..,L$.

F_{jr}^{v} Traffic flow assigned to the rth k-disjoint set of OD pair "j" to satisfy the demand λ_{jv}, $v=1,2,.,V; j=1,2,...,J; r=1,2,.., R_j(k)$, $k=2$ if $v<4$, otherwise $k=3$.

Q_{jq}^{g} FD Recovery flow assigned to the qth path of OD pair "j" following failure "g", $j=1,2,..,J; g=1,2,..,G; q=1,2,.., R_j^g(1)$.

W_i^v Working resources assigned to link "i" to satisfy modeling traffic associated with policy v, $i=1,2,..,L$, $v=1,2,..,V$.

W_i Total amount of working resources assigned to link "i", $i=1,2,..,L$.

D_i^v Dedicated backup resources assigned to link i, for traffic related policy v, $i=1,2,..,L$. $D_i^v \geq 0$ ($D_i^v=0$) if the policy "v" is (not) associated with dedicated backup resources, Clearly, $D_i^v=0$ for $v=2,3,5,7$.

D_i Total amount of dedicated backup resources assigned to link "i", $i=1,2,..,L$.

S_i^v Shared backup resources assigned to link "i", for traffic related to policy v, $i=1,2,..,L$.. Clearly, no shared backup resources are assigned to policies not associated with shared backup resources, thus, $S_i^v=0$ for policies $v=1,3$-6 while $S_i^v \geq 0$ for policies $2,7$-10. We divide the policies associated with shared resources into two groups: Group 1 - Policies 2, 9 and 10; and Group 2 - Policies 7 and 8.

Group 1 policies assign shared backup resources immediately after the "first" failure while Group 2 policies assign shared backup resources immediately after the "second" failure. This difference is taken into account by the following two variable sets:

$S_i^v(g)$ Shared backup resources assigned to link i, for traffic related Group 1 policies, $v=2,9,10; i=1,2,..,L$, following network failure "g", $g=1,2,..,G$.

$S_i^v(gh)$ Accumulated shared resources assigned to link i, for traffic related Group 1 policies, *v=7,8*; *i=1,2,..,L*, following the consecutive failures "*g,h*". The case *h=g* refers to a single-network-failure situation, thus, $S_i^v(gh) \geq S_i^v(gg)$, where *g,h=1,2,..,G*

S_i Total amount of shared backup resources assigned to link *i, i=1,2,..,L*. Two polar approaches may be considered about the way of calculating the shared resources:

The conservative approach - assigns separate shares resources to each policy;

The adaptive approach - uses the shared resources as a "pool" to serve all policies. Priority of using shared resources may also be applied to certain policies, especially during emergency scenarios. Based on the principle that shared resources are assigned to meet worst-case failure scenarios, the terms S_i can be calculated as follows:

For the conservative approach;

$$S_i = \sum_{v=1}^{10} S_i^v = \sum_{v=2,9,10} S_i^v + \sum_{v=7,8} S_i^v = \sum_{v=2,9,10} Max_{1\leq g\leq G}\{S_i^v(g)\} + \sum_{v=7,8} Max_{1\leq g,h\leq G}\{S_i^v(gh)\} \quad (3)$$

For the adaptive approach;

$$S_i = Max_{1\leq g\leq G}\{ \sum_{v=2,9,10} S_i^v(g) + \sum_{v=7,8} Max_{1\leq h\leq G}\{S_i^v(gh)\} \} \quad (4)$$

We formulate a generic network model, using the conservative approach, as follows:

M1: $Min \{ \sum_{i=1}^{L} C_i \cdot X_i \}$

S.t.

$$\sum_{v=1}^{10} (W_i^v + D_i^v + S_i^v) \leq \lfloor U \cdot M / 100 \rfloor \cdot X_i = \hat{M} \cdot X_i \qquad \forall i = 1,2,.., L \quad (5)$$

$$W_i^v, D_i^v, S_i^v, X_i \geq 0 \text{ and Integer}, \ \forall i = 1,2,.., L, \ v=1,2,..,V=10 \quad (6)$$

The above is a skeleton Integer Linear Programming (ILP) network model whose objective function minimizes total cost of transport equipment using a modified modularity value $\hat{M}$ that incorporates the utilization value *U*. Inequalities (5) indicate that the available resources on each link is used to support all types of traffic flows to meet working, dedicated and shared backup requirements. We assign D_i^v=0 if *v =2,3,5,7* and S_i^v=0 if *v=1,3-6,* ∀ *i=1,2,..,L,* appearing in inequalities (5), thus voiding irrelevant terms. To derive a complete network model, all terms appearing in inequality (5) are now elaborated.

We start with the single-failure policies, *v = 1,2,3:*

$$\sum_{r=1}^{R_j(2)} F_{jr}^{v} = \lambda_{jv} \qquad \forall v = 1,2,3; j=1,2,...,J \tag{7}$$

$$W_i^{v} = \sum_{j=1}^{J} \sum_{r=1}^{R_j(2)} \delta_{jr}^{i}(1,2) \cdot F_{jr}^{v} \qquad \forall v = 1,2; i=1,2,..,L \tag{8}$$

$$W_i^{3} = \sum_{m=1}^{2} \sum_{j=1}^{J} \sum_{r=1}^{R_j(2)} \delta_{jr}^{i}(m,2) \cdot F_{jr}^{3} \quad \forall\ i=1,2,..,L \tag{9}$$

$$D_i^{1} = \sum_{j=1}^{J} \sum_{r=1}^{R_j(2)} \delta_{jr}^{i}(2,2) \cdot F_{jr}^{1} \qquad \forall\ i=1,2,..,L \tag{10}$$

$$S_i^{2} \geq S_i^{2}(g) = \sum_{j=1}^{J} \sum_{r=1}^{R_j(2)} \delta_{jr}^{i}(2,2) \cdot \delta_{jr}^{g}(1,2) \cdot F_{jr}^{2} \qquad \forall\ i,g=1,..,L\ ,i \neq g \tag{11}$$

$$S_i^{2} \geq S_i^{2}(g) = \sum_{j=1}^{J} \sum_{r=1}^{R_j(2)} \delta_{jr}^{i}(2,2) \cdot \varepsilon_{jr}^{g-L}(1,2) \cdot F_{jr}^{2} \qquad \forall\ g=L+1,L+2,..,L+N;\ i=1,2,..,L \tag{12}$$

Constraints (7) - (12) are only associated with E2-DODP sets and $k=2$ appears as an index in the terms R, δ and ε. Constraints (7) satisfy traffic demand of policies $v=1\text{-}3$. Constraints (8) calculate working values on each link, taking into account that for policies $v=1,2$ the working paths are first within each 2-disjoint path sets. Constraints (9) only relate to Policy 3 for which the two paths of a selected set are designated to carry working flows.

Dedicated backup resources are associated with Policy 1 and the second path of a selected set, as in the constraints (10). Finally, constraints (11) and (12) refer to shared backup resources associated with Policy 2, using the second paths of selected sets if the first paths are affected by either link failures g, $g \leq L$, as in (11), or node failure $g\text{-}L$, $g>L$, as in (12). The inequality signs in both constrains (11) and (12) ensure that shared backup resources satisfy worst-case failure scenarios. To cope with double network failures, the terms $R_{j(3)}$ have to be used.

$$\sum_{r=1}^{R_j(3)} F_{jr}^{v} = \lambda_{jv} \qquad \forall v = 4,5,..,10;\ j=1,2,...,J \tag{13}$$

$$W_i^{v} = \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(1,3) \cdot F_{jr}^{v} \qquad \forall v = 4,7,8,9,10;\ \ i=1,2,..,L \tag{14}$$

$$W_i^{5} = \sum_{m=1}^{3} \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(m,3) \cdot F_{jr}^{5} \quad \forall\ i=1,2,..,L \tag{15}$$

$$W_i^6 = \sum_{m=1}^{2} \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(m,3) \cdot F_{jr}^{6} \quad \forall\ i=1,2,..,L \tag{16}$$

$$D_i^4 = \sum_{m=2}^{3} \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(m,3) \cdot F_{jr}^{4} \quad \forall\ i=1,2,..,L \tag{17}$$

$$D_i^6 = \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(3,3) \cdot F_{jr}^{6} \quad \forall\ i=1,2,..,L \tag{18}$$

$$D_i^v = \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(2,3) \cdot F_{jr}^{v} \quad \forall\ v=8,9,10\ ; i=1,2,..,L \tag{19}$$

Constraints (13) and (7) are quite similar, now using paths with $k=3$. Constraints (14) calculate the working capacity on each link, excluding Policies 5 and 6, taking into account that the working resources can only assigned to the first path of selected 3-disjoint sets. For Policies 6 and 5, working resources are also assigned to the second (Split+) and to the third (TWS) paths of selected sets, expressed by constraints (16) and (15), respectively. Policy 4 (TWP) is unique as dedicated backup resources are assigned to both second and third paths of selected sets, expressed by constraints (17). Constraints (18) indicate that Policy 6 uses dedicated backup resources through the third paths of selected sets. No dedicated resources are assigned to Policy 7. Dedicated backup resources are assigned to the second path of each selected set for the other policies, expressed by constraints (19).

Careful attention should be given to shared backup resources associated with compound failures. We start with Policy 7 (Policies 4 - 6 are not associated with shared backup resources).

$$S_i^7 \geq S_i^7(g) = \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(2,3) \cdot \delta_{jr}^{g}(1,3) \cdot F_{jr}^{7} \quad \forall\ i,g=1,..,L;\ i \neq g \tag{20}$$

$$S_i^7 \geq S_i^7(g) = \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(2,3) \cdot \varepsilon_{jr}^{g-L}(1,3) \cdot F_{jr}^{7} \quad \forall\ g=L+1,..,L+N;\ \ i=1,2,..,L \tag{21}$$

$$S_i^7 \geq S_i^7(g,h) = \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(3,3) \cdot [\delta_{jr}^{h}(2,3) + \varepsilon_{jr}^{h-L}(2,3)] \cdot \delta_{jr}^{g}(1,3) \cdot F_{jr}^{7} \quad \forall\ i,g \leq L\ , i \neq g;\ 1 \leq h \leq G \tag{22}$$

$$S_i^7 \geq S_i^7(g,h) = \sum_{j=1}^{J} \sum_{r=1}^{R_j(3)} \delta_{jr}^{i}(3,3) \cdot [\delta_{jr}^{h}(2,3) + \varepsilon_{jr}^{h-L}(2,3)] \cdot \varepsilon_{jr}^{g-L}(1,3) \cdot F_{jr}^{7} \quad \forall\ i \leq L;\ g > L;\ 1 \leq h \leq G \tag{23}$$

For Policy 7 (FI Dual shared), distinctions should be made due to the first network failure "*g*" for which resources are assigned to link *"i"* if it is along the second paths of 3-disjoint sets, expressed by constraints (20) and (21), and due to the consecutive failure "*h*", for which resources are assigned to link *"i"* if it is along the third paths, constraints (22) and

(23). Constraints (20) indicate that there are two conditions for assigning shared backup resources to link "*i*" following link-failure "*g*": (i) the link-failure "*g*" affects the working paths; (ii) the recovery paths pass link "*i*". Shared backup resources on link "*i*" are accumulated over all combinations of "*j*" and "*r*". Constraints (21) modify constraints (20) due to node-failure "*g-L*". Constraints (22) and (23) introduce a third condition related to failure "*h*" that affects the second paths within 3-disjoint path sets. The third condition covers the cases of either a link or a node failure along the second paths, making the terms $[\delta_{jr}^{h}(2,3)+\varepsilon_{jr}^{h-L}(2,3)]=1$

Shared backup resources for Policy 8 traffic are assigned only after two consecutive failures "*g*" and "*h*", affecting the first two paths (working and dedicated backup path). Constraints 24-27 cover all four combinations of link and node failures associated with the first two paths, given that shared backup resources from link *"i"* are used only if it is along the third path of the affected E3-DODP set *"r"* associated with pair *"j"*.

$$S_i^8 \geq S_i^8(g,h)=\sum_{j=1}^{J}\sum_{r=1}^{R_j(3)}\delta_{jr}^{i}(3,3)\cdot\delta_{jr}^{h}(2,3)\cdot\delta_{jr}^{k}(1,3)\cdot F_{jr}^{8} \quad \forall\ i,g,h\leq L;\ i\neq g,h \tag{24}$$

$$S_i^8 \geq S_i^8(g,h)=\sum_{j=1}^{J}\sum_{r=1}^{R_j(3)}\delta_{jr}^{i}(3,3)\cdot\varepsilon_{jr}^{h-L}(2,3)\cdot\delta_{jr}^{g}(1,3)\cdot F_{jr}^{8} \quad \forall\ i,g\leq L\ ;i\neq g\ ;1\leq h\leq G \tag{25}$$

$$S_i^8 \geq S_i^8(g,h)=\sum_{j=1}^{J}\sum_{r=1}^{R_j(3)}\delta_{jr}^{i}(3,3)\cdot\delta_{jr}^{h}(2,3)\cdot\varepsilon_{jr}^{g-L}(1,3)\cdot F_{jr}^{8} \quad \forall\ i,h\leq L\ i\neq h;\ g>L \tag{26}$$

$$S_i^8 \geq S_i^8(g,h)=\sum_{j=1}^{J}\sum_{r=1}^{R_j(3)}\delta_{jr}^{i}(3,3)\cdot\varepsilon_{jr}^{h-L}(2,3)\cdot\varepsilon_{jr}^{g-L}(1,3)\cdot F_{jr}^{8} \quad \forall\ i\leq L;\ g,h>L \tag{27}$$

All four constraint sets 24-27 are required to ensure adequate shared resources for worst-case failure scenarios. No overlap of constraints 25 and 26 (order of link and node failures matters).

Assignment of shared backup resources to Policy 9 traffic is done immediately after the failure "*g*", affecting either the first or second designated paths but not both. Constraints (28) and (29) refer to link and node failures, respectively. The terms in rectangle parenthesis may have the value of either "1"or "0" for each failure "*g*".

$$S_i^9 \geq S_i^9(g)=\sum_{j=1}^{J}\sum_{r=1}^{R_j(3)}\delta_{jr}^{i}(3,3)\cdot[\delta_{jr}^{g}(2,3)+\delta_{jr}^{g}(1,3)]\cdot F_{jr}^{9} \quad \forall\ i,g=12,..,L,\ i\neq g \tag{28}$$

$$S_i^9 \geq S_i^9(g)=\sum_{j=1}^{J}\sum_{r=1}^{R_j(3)}\delta_{jr}^{i}(3,3)\cdot[\varepsilon_{jr}^{g-L}(2,3)+\varepsilon_{jr}^{g-L}(1,3)]\cdot F_{jr}^{9} \quad \forall\ i=1,2,..,L;\ g=L+1,..,L+N \tag{29}$$

Assignment of shared resources to Policy 10 traffic follows Policy 9 considerations. Constraints (30) - (31) and constraints (32 - 33) refer to link and node failures, respectively. Constraints (30) and (32) satisfy recovery of the lost traffic following failure "*g*", taking into account that the values in the rectangle parenthesis are either "1" or "0" for any value "*g*".

Constraints (31) and (33) calculate shared backup resources Q following failure "g". The terms (1 - δ) are introduced to utilize not affected working and dedicated resources on link "i" if belonging to the affected paths (FD adaptation). For such situations double resource consumption on link "i" is avoided as the terms (1 - δ) get the value zero.

$$\sum_{q=1}^{R_j^g(1)} Q_{jq}^g = [\delta_{jr}^g(1,3) + \delta_{jr}^g(2,3)] \cdot F_{jr}^{10} \qquad \forall j=1,2,..,J,\ g=1,2,..,L,\ r=1,2,..,R_j(3) \tag{30}$$

$$S_i^{10} \geq S_i^{10}(g) = \sum_{j=1}^{J} \sum_{q=1}^{R_j^g(1,1)} \delta_{jq}^i(1,1) \cdot [\delta_{jr}^g(2,3) \cdot (1-\delta_{jr}^i(2,3)) + (1-\delta_{jr}^i(1,3)) \cdot \delta_{jr}^g(1,3)] \cdot Q_{jq}^g \quad \forall\ i,g \leq L,\ i \neq g \tag{31}$$

$$\sum_{q=1}^{R_j^g(1)} Q_{jq}^g = [\varepsilon_{jr}^{g-L}(1,3) + \varepsilon_{jr}^{g-L}(2,3)] \cdot F_{jr}^{10} \qquad \forall j=1,2,..,J,\ \ L+1 \leq h \leq L+N,\ r=1,2,..,R_j(3) \tag{32}$$

$$S_i^{10} \geq S_i^{10}(g) = \sum_{j=1}^{J} \sum_{q=1}^{R_j^k(1,1)} \delta_{jq}^i(1,1) \cdot [\varepsilon_{jr}^{g-L}(2,3) \cdot (1-\delta_{jr}^i(2,3)) + (1-\delta_{jr}^i(1,3)) \cdot \varepsilon_{jr}^{g-L}(1,3)] \cdot Q_{jq}^g \quad \forall\ i \leq L;\ g > L \tag{33}$$

$$F_{jr}^v \geq 0 \text{ and Integer } \forall\ v=1,2,3,\ r=1,2,..,R_j(2), j=1,2,..,J; \tag{34}$$

$$F_{jr}^v \geq 0 \text{ and Integer } \forall\ v=4,5,..,10;\ r=1,2,..,R_j(3);\ j=1,2,..,J; \tag{35}$$

$$Q_{jq}^g \geq 0 \text{ and Integer } \forall\ j=1,2,..J;\ g=1,2,..,G=L+N;\ \ q=1,2,..,R_j^g(1). \tag{36}$$

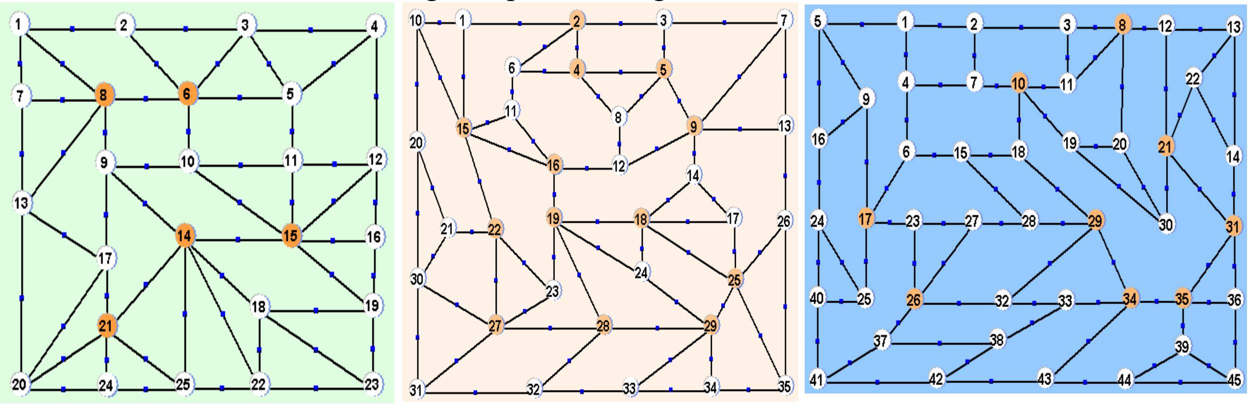
The above represents an ILP model. The boundary constraints (34-36) complement (7), referring now only to the non-negative flow variables. Policy 10 has a major impact on the number of model dimensions. Without Policy 10, the number of constraints does not exceed o(L^3), see that constraints 22 – 27 are *independent* of the set values $R_j(2)$ and $R_j(3)$. On the other hand, the number of variables is significantly larger, dependent on both $R_j(2)$ and $R_j(3)$, as can be seen in (34-36). Relaxation of the above model can be solved with no special difficulties even for huge transport networks by ordinary LP software packages (practically LP solutions are heavily dependent on the number of model constraints). This is a major advantage as lower-bound solutions and reference values used to evaluate the quality of feasible integer solutions can be obtained quite naturally. Introducing Policy 10 increases model constraints being dependent on $R_j(3)$ values, as can be seen by constraints (30) and (32). Model variables are increased as well, depending now also on the $R_j^k(1)$ values, see (36).

5. Numerical Examples

In this section we analyze three networks: Net25 - 25 sites, 50 fibers (AvND = 4.0); Net35 – 35 sites, 63 fibers (AvND = 3.6) and Net45 – 45 sites, 72 fibers (AvND = 3.2). The purpose is to present relative resource consumption of each policy under various network parameters. It can be seen that all sites in the three networks are interconnected by at least

Network Protocols and Algorithms
ISSN 1943-3581
2009, Vol. 1, No. 1

three fibers, thus satisfying the necessary conditions to cope with double network failures. Sites with above AvND are assigned special background colors.



(a) Net25 (b) Net35 (c) Net45

Figure 3 – Networks considered for analysis

For the sake of simplicity we use cost coefficients of transmission-system as link-independent and constant. The relative cost of each policy is derived by referencing as 100% the total cost found for the traditional Policy 1 (1+1 path protection) when the Ek-DODP sets are at the highest values considered (50 for all three ntworks). The testing parameters used are: (i) Number of Ek-DODP sets = 10, 20, 30, 40 and 50; (ii) Modularity value of transport systems M = 32, 48 and 64. We thus run the total of 450 different cases: For each of the three networks 150 cases are tested. Each case considers a single policy. End-to-end traffic is set in the range of 6-24, assigning higher values to neighboring OD pairs. We randomly select 50, 56 and 62 OD pairs with survivable traffic for Net25, Net35 and Net45, respectively, in a way that all network sites are actually associated with survivable traffic. AMPL and CPLEX versions 11.0 are used on a Pentium 4 with 2GB RAM machine, through a script prepared so as to carry out different runs in an automated manner. Figure 4 presents the results obtained for the various runs.

The following general observations can be ascertained from this extensive analysis:

I. **Double-network-failure policies**: Relative costs of policies that cope with double failures tend to increase in non-dense networks *more than* single-failure policies. Consider, for example, Policies 4, 8-10 appearing at the top of the graphs when using M = 32 (left graphs). The range of relative costs for these policies is 115-175, 130-200 and 140-205 in Net25, Net35 and Net45, respectively. Consider also Policy 6 (Split+) having relative costs less than 100 in Net25 and more than 100 in Net35 and Net45. A logical explanation is that E3-DODPs tend to be longer than E2-DODPs, especially in non-dense networks.

II. **Shared-backup-resource policies**: Relative costs associated with policies that rely on shared backup resources are *more sensitive* to the number of Ek-DODP sets compared to policies that rely on dedicated and dedicated-split backup resources. Consider, for example, the cost gaps between Policies 8-10 and Policies 1 and 6, which tend to decrease in all graphs when Ek-DODPs sets are increased. The most sensitive curves are associated with Policy 7 (dual-shared backup resources). It can be seen in Net35 and Net45 that the gap between Policy 7 and Policies 1&6 is quite small when selecting E3-DODP sets = 10. This gap is consistently increased in favor of Policy 7 upon using E3-DODP sets = 50. A logical explanation is that the efficiency of using shared backup resources increases with larger Ek-DODP sets as more backup paths may use the shared available resources. The practical aspects of this observation implies that for quality results it is recommended to select higher values of Ek-DODP sets when referring to policies with shared backup resources.

III. **Modularity value of transport systems**: Efficient use of resources is generally more demanding when employing large systems compared to the use of small systems. This is particularly true when the network load is low and the network itself is sparse. Consider, for example, Policies 2, 3 and 5, positioned at the bottom of the graphs of all networks. It can clearly be seen that the relative cost values associated with these three policies tend to increase when selecting higher modularity values and less-dense network, ranging 52-60 (Net25, M=32) and 64-84 (Net45, M=64).

We now refer specifically to each policy considered, trying to identify typical characteristics based on the results found. The relative cost values for the various cases represent the level of transport resources to be consumed with reference to the 1+1 path protection policy. For example, a relative cost of 80 implies that the specific case consumes only 80% of transport systems when compared to the 1+1 case.

1) Policy 1: The 1+1 Path-Protection policy is widely used in most telecommunication networks around the world. As can be seen in Figure 4, in terms of relative cost it is positioned more or less in the middle of the ten policy lines.

2) Policy 2: The SBPP policy requires the selection of at least 20 E2-DODP sets to reach quality results in terms of the efficient use of shared backup resources. The issue of bifurcation has been overlooked in our analysis. Relative cost values for this policy are 60 and 70 in dense and sparse networks, respectively.

3) Policy 3: Out of the ten policies detailed, the Split policy is at the lowest level. It may reach the relative cost value of 50, mainly in dense networks with low value of systems modularity.

4) Policy 4: TWP is placed at the relative higher cost level. It may reach the value of 200 mainly in sparse networks. High system modularity and high network density reduce the relative cost. Lower bound value is 150.

5) Policies 9 and 10: Differences between the two policies, in terms of resource utilization, are small. In sparse networks (Net45) the differences are even smaller and practically neglected. The use of FDPs in Policy 10 (part of the ASON standard), while increasing the number of model constraints and complexity of implementation, has not been found justified for the three test networks.

6) Policy 5: Relative TWS cost can be as low as 60 in dense networks that employ low-system modularity values (Net25, M = 32) and as high as 80 in less-dense networks that use high values of modularity systems (Net45, M = 64).

7) Policy 6: Split+ behaves similar to TWS but relative costs are higher by about 50% (the ratio of 1/2 over 1/3). The relative cost tends to decrease when using high M values.

8) Policy 7: The Dual-shared policy utilizes shared backup resources most efficiently. Despite coping with double network failures, this policy requires fewer network resources than the 1+1 policy. Selecting 20-40 E3-DODP sets is recommended for quality results.

9) Policy 8: Being part of policies which use shared backup resources, selecting at least 20 E3-DODPsets is recommended for quality results, especially when modularity of transport systems is high.

Network Protocols and Algorithms
ISSN 1943-3581
2009, Vol. 1, No. 1

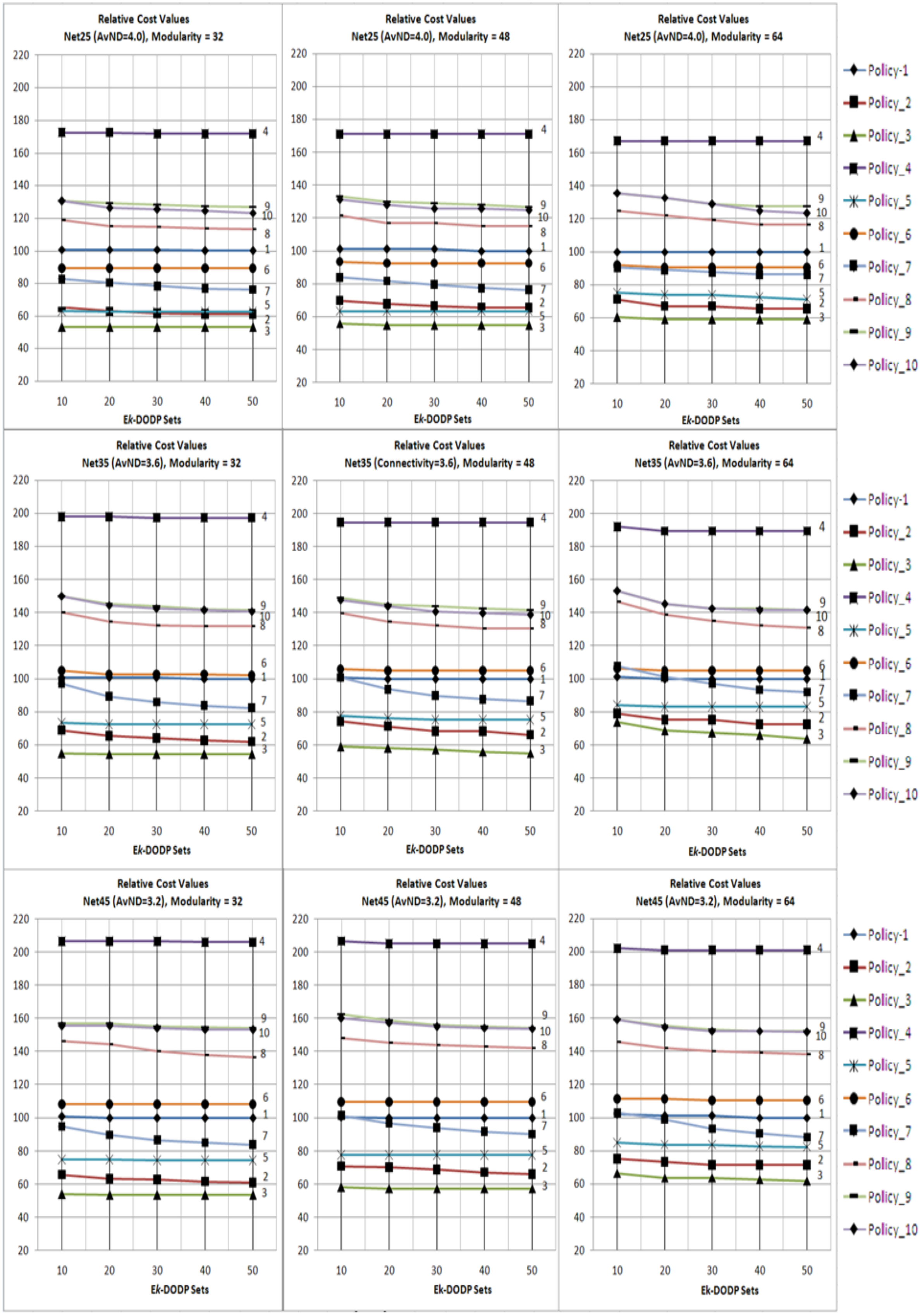


Figure 4 – Relative cost values found for the various cases tested

6. Summary and Conclusions

We present a general network paradigm suitable for a wide variety of survivability policies to cope with single and double-network failures, including node, link and multi-link instances. A sample of ten different survivability policies are detailed, each of which is unique in terms of complexity, resource consumption and recovery times. Based on the OD Cycles approach, a practical-oriented network model, which considers all ten policies discussed, has been developed and tested. Major cumulative advantages of the model, and the preliminary use of diverse-routing network algorithms to create an in-depth input data, enable supplying optimal solutions within a single computational process for any subset of policies considered. As a consequence, the model can be applied to quantify consumption of network resources associated with each policy for evaluation and customer-charging purposes. The impact of networks density (or AvND), number of Ek-DODP sets used and modularity of transport systems is widely investigated on three test networks. Network density is found to be the key factor for the efficient use of network resources, based on the following observations: (i) Network-cost differences between double and single-failure policies are not constant and decrease considerably in dense network; (ii) Quality results associated with policies that rely on shared backup resources require using larger number of Ek-DODP sets compared to policies that rely on dedicated and dedicated-split backup resources. This requirement is significantly more effective and achievable in dense networks; (iii) High modularity values of transport systems, which often yield economy-of-scale advantages, may notably affect resource utilization levels, especially when network loads are low. Network density is a major factor to alleviate that obstacle. The prolific use of a wide-variety of survivability policies is therefore shown to not only be service dependent but also network-density dependent.

References

[1] Bhandari R. (2002). Survivable Network Algorithms for Diverse Routing, *Kluwer Academic Press*

[2] Blake S. and Nadeau T. (Eds.) (1998). An Architecture for Differentiated Services, *IETF RFC 2475*

[3] Blouin F.J., Sack A., Grover W.D., Nasrallah H. (2003). Benefits of *p*-Cycles in a Mixed Protection and Restoration Approach, *Design of Reliable Com. Networks. DRCN'03*, pp.203-211

[4] Cholda P., Mykkeltveit A., Helvik B.E., Wittner O.J. and Jajszczyk A. (2007). A Survey of Resilience Differentiation Framework in Communication Networks, *IEEE Communications Surveys & Tutorial,* vol. 6, no. 4, pp. 32-55

[5] Dunn A.D., Grover W.D. & Macgregor M.H. (1994). Comparison of k-shortest Paths and Max-flow Routing for Network-facility Restoration, *IEEE JSAC*, vol.12, no.1, pp. 88-99

[6] Farkas A., Szigeti J. and Cinkler T. (2005). *P*-Cycles Based Protection Schemes for Multi-Domain Networks, *DRCN'05*, pp. 223-230

[7] Gerstel O. and Sasaki G. (2001). Quality of Protection (QoP): A Quantitative Unifying Paradigm to Protection Service Grades, *OptiComm*

[8] Gibbs N. E. (1969). A Cycle-generation Algorithm for Finite Undirected Linear Graphs, *Journal of Association for Computing Machinery*, vol.16, no. 4, 564-568

[9] Grover W. D. and Clouqueur M. (2003). Span Restorable Mesh Networks with Multiple Quality of Protection Service Classes, *Inter. Conference on Optical Com. and Network (ICON'02),* pp. 321-326

[10] Grover W. D. and Stamatelakis D. (1998). Cycle-oriented Distributed Reconfiguration: Ring-like Speed with Mesh-like Capacity for Self-healing Network Restoration, *ICC'98,* pp.537-543

[11] Guo L., Yu H., Li L. and Lou H. (2004). Shared Path-protection Algorithm for Dual-link Failures in Survivable WDM Mesh Networks, *International Conference on Parallel Processing Workshop (ICPPW'2004),* pp. 394-398

[12] He R., Lin B., Li L. and Gu C. (2005). Dynamic Shared Path Protection Algorithm in WDM Mesh Networks under Service Level Agreement Constraints, *International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'2005),* pp. 205-209

[13] Herzberg M. and Raz D. (2005). Resource Assignment in Multi-service Survivable Networks Based on the Cycle-oriented Approach, *International Teletraffic Congress (ITC19),* pp. 1621-1630

[14] Herzberg M., Shleifer F., Ring R. and Zolberg O. (2007). Applying OD Cycles to Multi-domain, Multi-service Survivable Networks, *3rd Euro-NGI Conference on Next Generation Internet Networks, Session on Robustness*

[15] Josza B.G., Orincsay D. and Kern A. (2003). Surviving Multiple Network Failures Using Shared Backup Path Protection, *IEEE International Symposium on Computers and Communication (ISCC'2003),* pp. 1333-1340

[16] Kodian A., Grover W. D. and Doucette J. (2005). A Disjoint Route-Sets Approach to Design of Path-Protecting *P*-Cycles Networks, *DRCN'05,* pp. 231-238

[17] Lakatos Z. (2003). Design of Automatically Switched Optical Networks, *5th International Conference on Transparent Optical Networks,* vol. 2, pp. 125-128

[18] Lee J.D., Kim S.U., Lee S.S., Jung J.I. and Su D.H. (2003). Differentiated Wavelength Assignment with QoS Recovery for DWDM Next Generation Internet Backbone Networks, *Photonic Network Communications,* vol. 5, no. 2, pp. 163-175

[19] Matthes N. and Lange R. (2002). Service Costs in a Convergent Network, *Networks*02, pp. 171-175

[20] Mukherjee C. Ou. (2005). Survivable Optical WDM Networks, *Springer US*

[21] Ricciato F., Listanti M. and Salsano S. (2004). An Architecture for Differentiated Protection Against Single and Double Faults in GMPLS, *Photonic Network Communications,* vol. 8, no. 1, pp. 119-132

[22] Sahin G. and Azizoglu M. (2003). Optical Layer Survivability for Single and Multiple Service Classes, *Journal of High-Speed Networks*, vol. 10, pp. 91-108

[23] Szigeti J., Gyarmati L. and Cinkler T. (2008). Multidomain shared protection with limited information via MPP and *p*-cycles, *Journal of Optical Networking*, vol. 7 no. 5, pp. 400-409

[24] Tacca M., Furmagalli A. and Unghvary F. (2003). Double-fault Path-Protection Scheme with Constrained Connection Downtime, 4th *International Workshop on the Design of Reliable Communication Networks (DRCN'2003),* pp. 181-188

[25] Xiong Y. and Mason L. (1999). Restoration Strategies and Spare-Capacity Requirements in Self-healing ATM Network, *IEEE/ACM Trans. on Networking*, vol. 7 no. 1, pp. 98-110