UNIVERSIDADE DE SÃO PAULO

ESCOLA DE ENGENHARIA DE SÃO CARLOS

DEPARTAMENTO DE ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

ANDRÉ LUIZ FERRAZ LOURENÇO

Técnicas de proteção e restauração em redes ópticas elásticas

São Carlos - SP

2015

ANDRÉ LUIZ FERRAZ LOURENÇO

TÉCNICAS DE PROTEÇÃO E RESTAURAÇÃO EM REDES ÓPTICAS ELÁSTICAS

Dissertação apresentada à Escola de Engenharia de São Carlos da Universidade de São Paulo para obtenção do título de Mestre em Ciências, Programa de Engenharia Elétrica

Área de Concentração: Telecomunicações

Orientador: prof. Dr. Amílcar Careli César

São Carlos - SP

2015

Trata-se da versão corrigida da dissertação. A versão original se encontra disponível na EESC/USP que aloja o Programa de Pós-Graduação de Engenharia Elétrica

AUTORIZO A REPRODUÇÃO TOTAL OU PARCIAL DESTE TRABALHO, POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE.

Lourenço, André Luiz Ferraz
Técnicas de proteção e restauração em redes ópticas
LL892t elásticas / André Luiz Ferraz Lourenço; orientador Amílcar Careli César. São Carlos, 2015.

Dissertação (Mestrado) - Programa de Pós-Graduação em Engenharia Elétrica e Área de Concentração em Telecomunicações -- Escola de Engenharia de São Carlos da Universidade de São Paulo, 2015.

1. redes ópticas elásticas. 2. proteção e restauração. 3. algoritmo RSA. 4. heurísticas. 5. balanceamento dinâmico de carga. 6. política de alocação. 7. restauração por contração de banda. 8. simulação de eventos discretos. I. Título.

FOLHA DE JULGAMENTO

Candidato: Engenheiro **ANDRÉ LUIZ FERRAZ LOURENÇO.**

Título da dissertação: "Técnicas de proteção e restauração em redes ópticas elásticas".

Data da defesa: 26/11/2015

Comissão Julgadora:	**Resultado:**
Prof. Associado **Amilcar Careli Cesar** **(Orientador)** (Escola de Engenharia de São Carlos/EESC)	APROVADO
Profa. Dra. **Mônica de Lacerda Rocha** (Escola de Engenharia de São Carlos/EESC)	Aprovado
Prof. Dr. **Luiz Henrique Bonani do Nascimento** (Universidade Federal do ABC/UFABC)	APROVADO

Coordenador do Programa de Pós-Graduação em Engenharia Elétrica:
Prof. Associado **Luis Fernando Costa Alberto**

Presidente da Comissão de Pós-Graduação:
Prof. Associado **Paulo César Lima Segantine**

Dedico este trabalho aos meus pais José Rubens e Rosane, a minha irmã Larissa, e a toda a minha família.

AGRADECIMENTOS

Gostaria de agradecer às pessoas importantes que foram essenciais para a conclusão de mais esta etapa em minha vida.

Agradeço aos meus pais, José Rubens e Rosane por ter apoiado em todas as minhas decisões e estarem sempre ao meu lado cuidando de mim com muito amor e carinho.

Ao orientador Dr. Amílcar Careli César, pelo exemplo de professor e pesquisador que me proporcionou esta oportunidade, orientando meu aprendizado.

A professora Dra. Mônica de Lacerda Rocha por ministrar uma das aulas mais importantes para o estudo de telecomunicações.

Aos demais docentes do departamento pelo conhecimento transmitido nas disciplinas ministradas.

Aos professores Dr. Washington Luiz e Dr. Maurício Figueiredo pela amizade e apoio durante e após a graduação.

A CAPES pela bolsa de estudos e ao CNPq pela aprovação do projeto que permitiu a obtenção de novos computadores para o laboratório.

A EESC-USP pela infraestrutura oferecida.

Aos meus companheiros de laboratório Rafael Jales, Nereida Valdívia, Natália Capelari e Arturo Miranda, por proporcionar um ambiente de amizade e reforçar o meu aprendizado.

Aos meus amigos de república, Pedro Oyama, Yuri Martins, Marcelo Barbosa e Daniel Sírio, por proporcionar um convívio saudável e momentos de alegria e descontração.

A Chien Ling Tseng, por todo amor e carinho que recebi ao longo dessa trajetória que me fez amadurecer e melhorar a cada dia praticando a paciência e a compreensão.

Watch your thoughts, for they become words.
Watch your words, for they become actions.
Watch your actions, for they become habits.
Watch your habits, for they become your character.
And watch your character, for it becomes your destiny.
What we think, we become.

1977 May 18, San Antonio Light, What They're Saying, Quote Page 7-B (NArch Page 28), Column 4, San Antonio, Texas. (NewspaperArchive)

RESUMO

LOURENÇO, A. L. F.. **Técnicas de proteção e restauração em redes ópticas elásticas**. 2015. Dissertação (Mestrado) – Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2015.

As redes ópticas estão passando por mudanças significativas, impulsionadas pelo crescimento exponencial do tráfego, principalmente advindo de serviços multimídia e armazenamento em nuvem. Esta demanda exigirá aumento da capacidade da taxa de transmissão para padrões como 400 Gb/s e 1 Tb/s. Nesse contexto, foi proposta uma arquitetura de rede com grade de frequências granular flexível chamada *elastic optical network* (EON). A EON divide o espectro de frequências em fatias (*slots*) de tamanho fixo e aloca grupos de slots contíguos estritamente de acordo com os requisitos de banda das demandas de conexão, implicando eficiência de uso do espectro. Com o aumento significativo da taxa de transmissão, acentuou-se a preocupação em manter a sobrevivência da rede, já que pouco tempo de queda no serviço pode acarretar uma imensa perda de dados. Neste trabalho, investigamos esquemas de proteção baseados em caminhos compartilhados (*shared-path protection, SPP*) e esquemas de restauração de tráfego. Avaliamos esquemas divulgados na literatura como o *dynamic load balancing shared-path protection* (DLBSPP) e esquemas de restauração como o *traffic aware restoration* (TAR) e *bandwidth squeezed restoration* (BSR). Avaliamos também uma heurística de alocação de slots chamada *inverted dual stack* (IDS). O DLBSPP utiliza balanceamento dinâmico de carga para computar os caminhos primários e de proteção compartilhados. O TAR executa a restauração dinâmica ordenando as conexões por granularidade de banda. O BSR utiliza a capacidade de contração de banda do EON para restaurar conexões por meio da política de melhor esforço ou de banda garantida, dependendo do acordo de níveis de serviço do cliente. O esquema IDS concentra o maior número possível de slots compartilhados em uma região do espectro. As medidas de desempenho dos algoritmos são avaliadas segundo as métricas: probabilidade de bloqueio, taxa de utilização do espectro, número médio de hops e taxa de restauração falha. As simulações computacionais mostram o bom desempenho da utilização do esquema IDS com DLBSPP.

Palavras-chave: Redes ópticas elásticas, proteção e restauração, algoritmo RSA, heurísticas, balanceamento dinâmico de carga, política de alocação, restauração por contração de banda, simulação de eventos discretos, processo de Poisson.

ABSTRACT

LOURENÇO, A. L. F.. **Protection and restoration techniques in elastic optical networks**. 2015. Dissertation (Master's Degree) – Engineering School of São Carlos, University of São Paulo, São Carlos, 2015.

Optical networks are undergoing significant changes driven by the exponentially growing traffic, especially coming from multimedia and cloud storage services. This demand will require increasing of the transmission rate capacity as high as 400 Gb/s and 1 Tb/s. Within this context, it was proposed the elastic optical network (EON), which is a network architecture with flexible granular frequency grid. EON divides the frequency spectrum into slices (slots) of fixed size and allocates groups of contiguous slots strictly according to the bandwidth requirement of the connection demands, providing high spectrum use efficiency. The significant increase in transmission rate put emphasis on the need to maintain the survival of the network, since the occurrence of faults in the network nodes or links can cause huge loss of data. In this work, we investigate protection schemes based on shared-path protection (SPP) and traffic restoration schemes. We evaluate schemes related in the literature, such as the dynamic load balancing shared-path protection (DLBSPP), and restoration schemes such as the traffic aware restoration (TAR) and the bandwidth squeezed restoration (BSR). The DLBP scheme uses dynamic load balancing to compute primary and shared protection paths. The TAR performs dynamic restoration ordering the connections based on band granularity. The BSR uses EON's band squeezing feature to restore connections by means of the best effort or guaranteed bandwidth strategy, depending on the customer's service level agreement. IDS scheme concentrates the maximum possible number of shared slots in a given region of the spectrum. Performance of the algorithms are evaluated according to metrics: blocking probability, spectrum utilization rate, average number of hops and failure restoration rate. Computer simulations show that the use of the IDS scheme improves the performance of the investigated algorithms.

Keywords: Elastic optical network, protection and restoration, RSA algorithm, heuristics, dynamic load balancing, allocation policy, bandwidth squeezed restoration, discrete event simulation, Poisson process.

LISTA DE FIGURAS

Figura 1 - Definição das bandas do espectro utilizado em comunicações ópticas. 37
Figura 2 - Alocação de banda em grade rígida de frequências com 50 GHz de espaçamento. 39
Figura 3 - Grade de espectro flexível. a) Nyquist, b) OFDM. 40
Figura 4 - Diagrama de blocos do *transponder*. Baseado em [18]. 41
Figura 5 - Associação entre fluxos de dados e caminhos ópticos em um S-BVT. Adaptado de [19]. 42
Figura 6 - ROADM construído com OXC [22]. 43
Figura 7 - Funcionamento do WSS [22]. 44
Figura 8 - Diagrama de funcionalidades do plano de controle. 48
Figura 9 – Comparação da alocação de banda. a) Grade fixa que mantém as bandas de guarda entre os caminhos ópticos que transmite duas demandas, uma de 100 Gbps e outra de 40 em uma grade rígida de frequências; b) os canais das demandas podem ser alocados em um espectro flexível provendo uma economia de 4 slots de frequência de espectro. Baseado em [14]. 52
Figura 10 - Nível de modulação e distância de transmissão para QoT aceitável. Adaptado de [5]. 53
Figura 11 – Representação de uma rede (nós A-B-C-D-E, enlaces L1, L2, L3, L4). São alocados três caminhos ópticos que atendem a três demandas de conexão. a) O tráfego de 400G alocado no caminho óptico 1 percorre uma distância de 1400 km e, neste caso, diminui-se a ordem do formato de modulação, b) outro tráfego de 400G alocado no caminho óptico 2 percorre uma curta distância (200 km) que permite a utilização de um formato de modulação de mais alta ordem, e c) o tráfego de 100G alocado no caminho óptico 3 percorre uma distância intermediária (400 km), portanto um formato de modulação intermediário é selecionado. 54
Figura 12 - Fragmentação do espectro: a) espectro ocupado; b) espectro central liberado; c) alocação de um novo espectro não encaixa na lacuna formada, realocada em outra faixa espectral (lacuna inutilizada); d) outro espectro é liberado; e) a conexão não se encaixa em nenhuma das duas lacunas deixadas e é bloqueada. 56
Figura 13 - Classificação dos esquemas de gerenciamento de falha, adaptado de [35] 58
Figura 14 – Proteção baseada em enlace: a) um enlace de proteção dá suporte ao enlace entre os nós 1 e 2; e b) uma falha no enlace entre os nós 1 e 2 interrompe a conexão representada pela linha pontilhada, e a conexão é reestabelecida pelo enlace de proteção. 58
Figura 15 – Restauração baseada no enlace. a) A conexão estabelecida não tem suporte com enlace de proteção; e b) em caso de falha no enlace entre os nós 1 e 2, uma nova rota é estabelecida em torno do enlace da falha. 59
Figura 16 – Proteção baseada em caminho. a) um caminho de proteção (pontilhado cinza) dá suporte a um caminho de trabalho; e b) uma falha no enlace entre os nós 1 e 2 interrompe o caminho de trabalho e o fluxo é encaminhado para o caminho de proteção. 59
Figura 17 – Restauração baseada em caminho. a) um caminho de trabalho desprotegido; b) ocorre uma falha no enlace entre os nós 1 e 2 que interrompe o caminho de trabalho e uma rota alternativa pode ser traçada utilizando os enlaces disponíveis indicados em verde; c) um caminho de recuperação com mesmo número de saltos é escolhido; d) um caminho de recuperação mais longo é escolhido. 60
Figura 18 – Restauração baseada em subcaminho. a) um caminho de trabalho desprotegido; b) uma falha no enlace entre os nós 7 e 8 interrompe o caminho de trabalho e os possíveis enlaces que podem constituir a rotas a partir do nó anterior à falha são explicitados; c) um

subcaminho é computado entre os nós 7 e 8; d) outro subcaminho com número maior de saltos é computado. 61
Figura 19 – Exemplos de DPP. a) Configuração DPP 1+1, o sinal é transmitido para a o caminho primário (P1) e secundário (S1) da demanda de conexão (C1). b) Configuração DPP 1:1, o sinal é transmitido apenas para o caminho primário (P1), o caminho secundário mantém-se reservado. 62
Figura 20 - Exemplo SPP, o caminho secundário (de proteção compartilhada) S1 protege os caminhos primários P1 e P2 das conexões C1 e C2. 63
Figura 21 - Exemplo de estabelecimento de um SPP. a) duas demandas de conexão C1 e C2 utilizam dois caminhos primários P1 e P2 e um caminho de proteção compartilhada S1; b) uma nova demanda de conexão C3 é alocada no caminho primário P3; e c) um caminho de proteção S2 é encontrado para P3. 65
Figura 22 – Exemplo de proteção SPP na ocorrência de uma única falha. a) as demandas de conexão alocadas conforme a Fig.21c; b) uma falha ocorre no enlace entre os nós 4 e 7; e c) os caminhos de proteção S1 e S2 são ativados e restauram as conexões. 66
Figura 23 - Exemplo de SPP. a) *conservative sharing policy*; e b) *aggressive sharing policy*. 67
Figura 24 - Exemplo da restauração TAR. a) conexões C1 e C2; e b) as conexões C1 e C2 são recuperadas como R1 e R2 e os espectros alocados de acordo com prioridade de tráfego. Adaptado de [8]. 68
Figura 25 – Níveis de serviço na alocação. a) FBGR com restauração completa. b) PBGR com 50% de contração de banda. c) BER, não há proteção reservada. Adaptado de [10]. 70
Figura 26 - Representação dos grafos: a) por matriz de adjacência e b) por lista de adjacência. 76
Figura 27 - Exemplo de balanceamento de carga para alocação do caminho primário do nó fonte 1 ao nó destino 7. Dada uma topologia de rede inicial têm-se: a) alocação do menor caminho utilizando custo básico em cada enlace; b) alocação do menor caminho com os custos balanceados por (1). 78
Figura 28 - Caminhos disjuntos em: a) nó, b) enlace. 79
Figura 29 - Modificação da matriz de adjacência para obtenção de caminhos disjuntos em: a) nó e b) enlace. 80
Figura 30 - Abstração em blocos do espectro granular. 81
Figura 31 - Exemplo de alocação FF. a) alocação de 1 FSU, b) alocação de 2 FSUs, c) alocação de mais 2 FSUs , d) a alocação vermelha de 2 FSUs é liberada. e) uma demanda de 4 FSUs é alocado no primeiro conjunto livre que acomoda a demanda. f) a demanda de 3 FSUs não cabe no espectro é bloqueada. 82
Figura 32 - Alocação de espectro considerando múltiplos enlaces. a) Estado inicial de alocação dos enlaces. b) Alocação de duas demandas de conexão. 83
Figura 33 - Alocação de espaço de uma pilha e um segmento de dados em crescimento. Retirada de [42]. 84
Figura 34 - Funcionamento da heurística IDS. 85
Figura 35 - Alocação de caminhos (P)rimários e (S)ecundários com SPP ASP. 86
Figura 36- Alocação de caminhos (P)rimários e (S)ecundários com SPP ASP IDS. 86
Figura 37 - Atributos da entidade Nó. 89
Figura 38 - Entidade Enlace e seus atributos. 90
Figura 39 - Entidade FSU e seus atributos. 90
Figura 40 - Entidade Conexão e seus atributos. 91
Figura 41 - Interligações entre Nós e Enlaces. 92
Figura 42 - Banda do enlace composta de FSUs. 93
Figura 43 - Estado inicial de uma unidade de rede (2 Nós, 1 Enlace). 93

Figura 44 - Estado da unidade de rede após um atendimento de Conexão (Alocação da demanda). 94
Figura 45 - Evento e seus atributos. 95
Figura 46 - Fluxo de atividades para o evento de chegada de conexão. 97
Figura 47 - Fluxo de atividades para o evento partida de conexão. 98
Figura 48 - Fluxo de atividades para o evento de ocorrência de falha. 99
Figura 49 - Fluxo de atividades para o evento de restauração de falha. 99
Figura 50: Chegada e partida das conexões [45]. 101
Figura 51 - Diagrama simplificado de geração de eventos de chegada e partida de conexão 103
Figura 52 - Janela de operação para inserção de falhas 105
Figura 53 - Diagrama simplificado de geração de eventos de ocorrência e reparação de falha 106
Figura 54: Topologia de rede NSFNET [8] 109
Figura 55: Topologia de rede USNET [8]. 109
Figura 56 - Regiões de carga baixa e carga alta de tráfego. 113
Figura 57 - Gráfico de BP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET. 115
Figura 58 - Gráfico de SUR comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET. 117
Figura 59 - Gráfico de *Primary* AHOP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET. 119
Figura 60 - Gráfico de *Backup* AHOP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET. 120
Figura 61 - Gráfico de AHOP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET. 122
Figura 62 - Gráfico de FRR comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET. 124
Figura 63 - Gráfico de SUR comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET. 126
Figura 64 - Gráfico de AHOP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET. 128
Figura 65 - Gráfico de *Primary* AHOP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET. 129
Figura 66 - Gráfico de Backup AHOP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET. 130
Figura 67 - Gráfico de FRR comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET. 132
Figura 68 - Gráfico de FRR comparando DR x TAR: a) NSFNET; b) USNET. 135
Figura 69 - Gráfico de BP comparando BSR x DR: a) NSFNET; b) USNET. 137
Figura 70 - Gráfico de SUR comparando BSR x DR: a) NSFNET; b) USNET. 139
Figura 71 - Gráfico de AHOP comparando BSR x DR: a) NSFNET; b) USNET. 141
Figura 72 - Gráfico de FRR comparando BSR x DR: a) NSFNET; b) USNET. 143
Figura 73 - Gráfico de BP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET. 145
Figura 74 - Gráfico de SUR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET. 147
Figura 75 - Gráfico de AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET. 149
Figura 76 - Gráfico de *Primary* AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET. 150

Figura 77 - Gráfico de *Backup* AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET. 151
Figura 78 - Gráfico de FRR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET. 153
Figura 79 - Gráfico de FRR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET. 155
Figura 80 - Gráfico de BP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET. 175
Figura 81 - Gráfico de BP comparando DR x TAR: a) NSFNET; b) USNET. 177
Figura 82 - Gráfico de SUR comparando DR x TAR: a) NSFNET; b) USNET. 178
Figura 83 - Gráfico de AHOP comparando DR x TAR: a) NSFNET; b) USNET. 179
Figura 84 - Gráfico de BP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET. 181
Figura 85 - Gráfico de SUR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET. 182
Figura 86 - Gráfico de AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET. 183

LISTA DE TABELAS

Tabela 1 - Previsão de crescimento da demanda de banda de 2014 a 2019 30
Tabela 2 - Tecnologias que habilitam EONs de 400G/1T..... 32
Tabela 3 - Formatos de modulação 53
Tabela 4: Variáveis utilizadas pelo algoritmo DLBSPP [8]..... 77
Tabela 5 - Entidades principais do modelo de rede..... 88
Tabela 6 - Tipos de Eventos 95
Tabela 7 - Significado dos atributos para cada tipo de evento. 96
Tabela 8 – Limite superior teórico de AHOP..... 107
Tabela 9 - Grupo 1: Comparação entre SPP e DPP, com e sem restauração dinâmica..... 111
Tabela 10 - Grupo 2: Comparação entre Restauração dinâmica e restauração TAR 111
Tabela 11 - Grupo 3: Restauração BSR em diferentes proporções de níveis de serviço. 112
Tabela 12 - Grupo 4: Comparação SPP, DLBSPP, SPP+IDS, DLBSPP+IDS sem restauração 112
Tabela 13 - Grupo 5: Comparação SPP, DLBSPP, SPP+IDS, DLBSPP+IDS com restauração 112
Tabela 14 - Quantidade total de recursos alocados para os esquemas DPP e SPP sem restauração(x 1 milhão). 118
Tabela 15 - Quantidade total de recursos alocados para os esquemas DPP e SPP sem restauração (x 1 milhão). 127
Tabela 16 - Quantidade total de recursos alocados para os esquemas DPP e SPP com restauração (x 1 milhão). 127
Tabela 17 - Ganho relativo percentual de FRR entre os esquemas sem restauração e com restauração 133
Tabela 18 - Quantidade total de recursos alocados para os esquemas com restauração BSR e DR..... 140
Tabela 19 - Quantidade total de recursos alocados para os esquemas SPP, DLBSPP, SPP IDS e DLBSPP IDS (x 1 milhão). 148
Tabela 20 - Ganho relativo percentual de FRR entre os esquemas SPP, DLBSPP, SPP IDS e DLBSPP IDS. 156

LISTA DE ABREVIATURAS

ADR	*add drop regenerators*
ASP	*aggressive sharing policy*
AHOP	*average hop*
BER	*best effort recovery*
BFS	*breadth-first search*
BGP	*border gateway protocol*
BP	*blocking probability*
BSR	*bandwidth squeezing restoration*
BV-T	*bandwidth variable-transponder*
BV-WSS	*bandwidth variable-wavelength selective switct*
CA	carga alta
CAGR	*compound annual growth rate*
CB	carga baixa
CD	*cromatic dispersion*
DLB	*dynamic load balancing*
DLBSPP	*dynamic load balancing shared-path protection*
DR	*dynamic restoration*
DSP	*digital signal processing*
DPP	*dedicated path protection*
DWDM	*Dense WDM*
EDFA	*erbium doped fiber amplifier*
EON	*elastic optical network*
FBGR	*full bandwidth guaranteed recovery*
FEC	*forward error correction*
FF	*first-fit*
FIFO	*first in first out*
FRR	*failure restoration ratio*
FSU	*frequency slot unit*
GMPLS	*generalized multiprotocol label switching*
IDS	*inverted dual stack*
IGP	*interior gateway protocol*

ITU	*International Telecommunication Union*
LCoS	*liquid crystal on silicon*
LIFO	*last in first out*
LMP	*link management protocol*
MB-OFDM	*multi-band* OFDM
MEMS	*micro-electro-mechanical systems*
MPLS	*multiprotocol label switching*
NP	*nondeterministic polynomial-time*
NP-hard	*non-deterministic polynomial-time hard*
O-OFDM	*optical* OFDM
OADM	*optical add-drop multiplexer*
OEO	*optical-eletro-optical*
OFDM	*orthogonal frequency division multiplexing*
OPM	*optical performance monitor*
OSNR	*optical signal-to-noise ratio*
OSPF-TE	*open shortest path first with traffic engineering*
OTDM	*orthogonal time division multiplexing*
OXC	*optical cross connector*
PBGR	*partial bandwidth guaranteed recovery*
PCE	*path computation element*
PMD	*polarization mode dispersion*
QoT	*quality of transmission*
QPSK	*quadrature phase shift keying*
ROADM	*reconfigurable optical add drop multiplexer*
RS	*random service*
RSA	*routing and spectrum assignment*
RWA	*routing and wavelength assignment*
RSVP-TE	*resource reservation protocol with traffic engineering*
S-BVT	*sliceable* BVT
SDN	*software defined network*
SLA	*service level agreement*
SLICE	*spectrum-sliced elastic optical path*
SPP	*shared protection path*
SUR	*spectrum utilization ratio*

TAR	*traffic aware restoration*
WDM	*wavelength division multiplexing*
WSS	*wavelength selective switch*

SUMÁRIO

1 INTRODUÇÃO 29
2 REDES ÓPTICAS ELÁSTICAS 37
2.1 O espectro elástico: escalabilidade e flexibilidade 37
2.2 Arquitetura de nós 41
2.3 O problema de roteamento e alocação de espectro 44
2.4 Plano de Controle 46
2.4.1 Protocolo de Roteamento 49
2.4.2 Protocolo de Sinalização 49
2.5 Características principais do EON 51
2.5.1 Eficiência espectral 51
2.5.2 Distância adaptativa 52
2.5.3 Gerenciamento eficiente de energia 54
2.5.4 Fragmentação do Espectro 55
3 ESQUEMAS DE PROTEÇÃO E RESTAURAÇÃO 57
3.1 Classificação dos esquemas 57
3.1.1 Atuação em enlace 58
3.1.2 Atuação em caminho 59
3.1.3 Atuação em subcaminho 60
3.2 *Proteção de caminho dedicado* (DPP) 1+1/1:1 61
3.3 *Proteção de caminho compartilhado* (SPP) 1:N 63
3.3.1 SPP *aggressive sharing policy* (ASP) 66
3.4 *Traffic-aware restoration* (TAR) 67
3.5 *Bandwidth squeezing restoration* (BSR) 68
4 ALGORITMOS RSA 73
4.1 O subproblema de roteamento 73
4.1.1 O algoritmo de Dijkstra 74
4.1.2 Dynamic load balancing shared-path protection (DLBSPP) 76
4.1.3 Obtenção dos caminhos disjuntos 78
4.2 O subproblema de alocação de espectro 80
4.2.1 Algoritmo *first fit* (FF) 81
4.2.2 Inverted dual stack (IDS) 83
5 SIMULAÇÃO 87
5.1 Modelagem da Simulação 87
5.1.1 Modelo de rede 88

5.1.2 Modelo do plano de controle 94
5.1.3 Modelo de geração de tráfego e de falhas 99
5.2 Métricas Utilizadas 107
5.3 Formulação do Problema 109
6 ANÁLISE DOS RESULTADOS 113
6.1 Resultados do Grupo 1 – SPP x DPP 114
6.1.1 Para uma única falha 114
6.1.2 Para três falhas simultâneas 125
6.2 Resultados do Grupo 2 – Restauração Padrão x TAR 133
6.3 Resultados do Grupo 3 – BSR x DR 136
6.4 Resultados do Grupo 4 – SPP x DLBSPP x SPP IDS x DLBSPP IDS com comutação de caminhos 144
6.5 Resultados do Grupo 5 – SPP x DLBSPP x SPP IDS x DLBSPP IDS com restauração dinâmica 154
7 CONCLUSÕES 157
REFERÊNCIAS 161
APÊNDICE A – Pseudocódigo do algorito de *DIJKSTRA* 165
APÊNDICE B – Pseudocódigo do algorito *first-fit* 167
APÊNDICE C – Pseudocódigo do algoritmo Caminho de trabalho 169
APÊNDICE D – Pseudocódigo do algoritmo *DPP* 171
APÊNDICE E – Pseudocódigo do algoritmo *SPP* 173
APÊNDICE F – Gráfico BP do experimento G1 para 3 falhas 175
APÊNDICE G – Gráficos BP, SUR e AHOP do experimento G2 177
APÊNDICE H – Gráficos BP, SUR e AHOP do experimento G5 181

1 INTRODUÇÃO

Os recentes sistemas de transmissão WDM de 40 Gbps (40G) e 100 Gbps (100G) para transmissão de longa distância têm sido implantados durante essa década no lugar dos sistemas WDM de 10 Gbps empregados na última década. As tecnologias que permitiram essas inovações foram: introdução de formatos de modulação multinível de fase, por exemplo, *quadrature phase shift keying* (QPSK), técnicas de multiplexação por divisão de polarização, detecção coerente, e equalização digital no domínio eletrônico juntamente com a amplificação óptica avançada. Essas tecnologias permitiram não só aumentar a eficiência espectral, como também a distância de transmissão, mesmo se aplicadas na infraestrutura de fibras implantadas desde a década de 1990 [1].

Essa mudança tecnológica vem ocorrendo devido ao aumento crescente da demanda por largura de banda. A Tabela 1 mostra a previsão do aumento do tráfego IP global entre os anos de 2014 a 2019. Em 2014 o tráfego global era de 59.848 Petabytes/mês, em 2019 a previsão é que o tráfego global atinja 167.978 Petabytes/mês. Uma medida utilizada para expressar a taxa anual de crescimento sobre um período de tempo é o *compound annual growth rate* (CAGR)[1]. O CAGR para o tráfego IP global entre os anos de 2014 a 2019 é de 23%, isso significa que a demanda por banda praticamente dobra a cada 4 anos ($1{,}23^4 = 2{,}28$) [2].

Um dos principais motivos para o aumento da demanda é o aumento do mercado de dispositivos móveis e também de tecnologias de transmissão de dados móveis como o 3G e o 4G. Segundo a Tabela 1, o aumento da demanda sobre dados móveis é a maior dentre as outras, com 57% de CAGR. Outros motivos relevantes é a popularização das transmissões de vídeo em alta definição (*Full HD*) e o aumento dos serviços de armazenamento e compartilhamento de arquivos em nuvem. Estes últimos contribuem tanto para o aumento do tráfego de internet fixa (CAGR 23%) como também de dados móveis, já que a maior parte dos dispositivos móveis do mercado permite acessar conteúdo multimídia com facilidade.

Os serviços de *Managed IP* consistem uma gama de serviços corporativos fornecidos por operadores de rede, provedores de serviços gerenciados e integradores de sistemas, que gerenciam aplicativos que funcionam através de redes IP da empresa cliente, como: telefonia IP, centros de contato IP, comunicações unificadas, hospedagem de aplicativos, segurança e

[1] Calculado por $CAGR(t_n, t_0) = \left(\frac{V(t_n)}{V(t_0)}\right)^{\frac{1}{t_n - t_0}} - 1$, em que V é o valor, t é o tempo

suporte remoto. Para esses serviços há uma previsão de 13% de CAGR, pois cada vez mais as empresas estão reduzindo o número de profissionais contratados na área de tecnologia de informação e terceirizando suas operações de rede.

Tabela 1 - Previsão de crescimento da demanda de banda de 2014 a 2019

	2014	**2015**	**2016**	**2017**	**2018**	**2019**	**CAGR 2014-2019**
Total (PB por mês)							
Tráfego IP Total	59.848	72.426	88.427	108.988	135.484	167.978	23%
Por Categoria (Petabytes [PB] por mês)							
Internet Fixa	39.909	47.803	58.304	72.251	90.409	111.899	23%
Managed IP	17.424	20.460	23.371	26.087	29.274	31.858	13%
Dados Móveis	2.514	4.163	6.751	10.650	16,124	24.221	57%
Por Segmento (PB por mês)							
Consumidor	47.740	58.137	71.453	88.730	111.015	138.415	24%
Empresarial	12.108	14.289	16.973	20.258	24.469	29.563	20%

Fonte: Cisco Visual Networking Index: Forecast and Methodology, 2014–2019 [2]

No entanto, o aumento crescente da demanda por largura de banda gera uma perspectiva de redução de capacidade nos próximos dez ou quinze anos e isso obriga os provedores de serviços a considerarem sistemas de transmissão com capacidade além de 100G, por exemplo, de 400 Gbps (400G) e 1 Tbps (1T), sendo que o formato de transmissão de 400G provavelmente será o primeiro padrão da próxima geração de redes ópticas. O processo de padronização deve considerar alguma compatibilidade com as tecnologias anteriores, principalmente com as fibras instaladas que possuem maior custo de reimplantação. Porém, a atualização das redes WDM para transmissões de 400G e 1T apresenta um problema de não ser flexível em escala devido ao modelo de grade fixa de frequências adotada. Este modelo de grade é padronizada pelo *International Telecommunication Union* (ITU) com espaçamentos que vão desde múltiplos de 100 GHz a 12,5 GHz, sendo o padrão de 50 GHz o mais popularizado nas redes ópticas de 40G e 100G.

As grades de frequências são configuradas nos equipamentos terminais, como o *optical add drop multiplexer* (OADM) e o *reconfigurable optical add drop multiplexer* (ROADM). Tanto o OADM quanto o ROADM são equipamentos que efetuam a comutação dos comprimentos de onda, no entanto, o ROADM possui funcionalidades adicionais que permitem reconfiguração remota da comutação dos comprimentos de onda e pode assumir mais de um padrão de grade que é selecionável em sua configuração. Mesmo com essa flexibilidade, a largura máxima do espectro ocupada pelo canal é limitada de acordo com a grade selecionada.

A utilização de formatos de modulação de mais alta ordem provê maior eficiência espectral proporcionando uma largura espectral modulada menor, mas as estreitas distâncias entre símbolos são mais susceptíveis a ruídos que degradam a relação sinal-ruído do sinal óptico e diminui a sua distância de transmissão. Por outro lado, os formatos de modulação de mais baixa ordem possuem largura espectral modulada maior e permitem maior distância de transmissão. Essa relação de compromisso entre "eficiência espectral" e "distância de transmissão" é limitada pelo espaçamento da grade utilizada. Por exemplo, considere um sistema de transmissão WDM de 400G com modulação DP-16QAM que na prática ocupa uma largura espectral de 80 GHz [1]. A largura espectral gerada não cabe em uma grade de 50 GHz, seria preciso então de uma grade com no mínimo 100 GHz de espaçamento. Caso o equipamento de rede não suporte a mudança de grade, não seria possível alocar o canal. Por outro lado, se a grade de 100 GHz fosse selecionada haveria um desperdício de 20 GHz de espectro. O desperdício poderia ser ainda maior caso houvesse canais que atendesse demandas de conexão menores que 400G, uma vez que tráfegos de menores taxas ocupam uma largura espectral menor. A solução proposta para contornar esses problemas é adotar o modelo de grade flexível e com menores espaçamentos (por exemplo, espaçamentos de frequência de 12,5 GHz, 6,25 GHz e menores) ao invés da grade fixa. A arquitetura de rede que emprega o modelo de grade flexível de frequências é chamada de *spectrum-sliced elastic optical path* (SLICE), conhecida de modo geral como *elastic optical network* (EON).

A ideia chave da EON é alocar os recursos espectrais necessários de acordo com demandas de tráfego. A menor unidade de banda do EON é chamada de subportadora, em que é alocada uma demanda de conexão a baixas taxas, permitindo que o sinal modulado tenha alta tolerância contra efeitos de dispersão cromática (*cromatic dispersion*, CD) e dispersão de modo de polarização (*polarization mode dispersion*, PMD) da fibra. A EON permite também a agregação na camada óptica responsável por formar o supercanal óptico. Dessa maneira a EON proporciona eficiência espectral e elasticidade [3]. Duas classes de tecnologias que podem abrir caminho para EONs de 400G e 1T: WDM-Nyquist e *multi-band orthogonal*

frequency division multiplexing (MB-OFDM) [1]. Na Tabela 2 mostra-se um conjunto de tecnologias que viabilizam EONs de 400G e 1T.

Tabela 2 - Tecnologias que habilitam EONs de 400G/1T

Tecnologia	**Objetivo**
Amplificadores de espectro mais amplo	Aumentar o espectro total utilizável
Amplificadores de ruído mais baixo	Aumentar a distância de transmissão
Novos tipos de fibra óptica	Reduzir a atenuação, dispersão do sinal e efeitos não lineares.
Projetos de novos WSS ROADM elásticos (3,125 ~ 6,250 GHz)	Permitir espectro mais granular/elástico
Mais formatos de modulação de alto nível	Melhorar a eficiência espectral
Melhoria da FEC	Melhorar a taxa de erros de *bits* na decodificação dos dados
Técnicas de geração de multiportadoras	Formação de subportadoras e supercanal óptico
Laser com largura de linha estreita	Diminuir os espaçamentos da grade
Digital Signal Processing (DSP)	Mitigar os efeitos não lineares da fibra

Um dos níveis de abstração de redes é o plano de controle, que cuida da gerência de tráfego da rede composto pelas demandas de conexão que são atendidas e alocadas na camada óptica. Diferentemente das redes no domínio elétrico que realizam comutação de pacotes, as redes ópticas funcionam com comutação de circuitos que estabelece previamente um caminho fim-a-fim antes que os dados sejam enviados. Isso garante que, após a conexão ter sido efetuada, não haverá congestionamento e os dados serão enviados de forma ordenada. Entretanto, configurar um caminho com antecedência provoca reserva e provável desperdício de largura de banda (redes WDM) [4].

Nas redes ópticas o circuito reservado é chamado de caminho óptico, que na arquitetura WDM corresponde a um comprimento de onda contínuo enquanto na arquitetura

EON corresponde a uma porção de espectro contínuo. Dessa maneira, o roteamento de tráfego que na arquitetura WDM era tratado como um problema de *routing and wavelength assignment* (RWA) torna-se um problema de *routing and spectrum assignment* (RSA), que em geral tem complexidade de tempo polinomial não determinístico (*non-deterministic polynomial-time*, NP) e é considerado um problema difícil (NP-*hard*) e, por esse motivo, quase sempre se adotam abordagens heurísticas para a solução. O problema RSA pode ser resolvido com algoritmos que encontram a solução conjunta, o "*joint*-RSA", ou separando-os em dois subproblemas: o de roteamento e o de alocação de espectro, o que diminui a complexidade e permite obter uma solução próxima da ótima. Alguns algoritmos RSA foram propostos em [5-7]. Nesse trabalho, foi utilizado o algoritmo RSA composto pelo algoritmo de *Dijkstra* para resolver o subproblema de roteamento e pelo algoritmo *first-fit* para resolver o subproblema de alocação de espectro.

Devido ao aumento significativo das taxas de transmissão previstas para EONs, uma das maiores preocupações do plano de controle é manter a sobrevivência da rede, já que pouco tempo de queda no serviço pode acarretar uma imensa perda de dados. Quando ocorre uma falha em um nó ou enlace, os esquemas de proteção e restauração garantem a sobrevivência da rede permitindo o restabelecimento das conexões por meio de outros nós e enlaces da rede. Um esquema de proteção reserva recursos prévios na rede, chamado de caminho de proteção ou caminho secundário. Um esquema de restauração procura alocar um novo caminho de trabalho para as conexões sejam reestabelecidas imediatamente após a ocorrência da falha. Esse trabalho aborda alguns esquemas de proteção e restauração presentes na literatura para EONs, como o esquema de proteção de caminho compartilhado com balanceamento dinâmico de carga (*dynamic load balancing shared-path protection*, DLBSPP) com restauração ciente do tráfego, (*traffic aware restoration*, TAR) [8] e o esquema de restauração por contração de banda (*bandwidth squeezing restoration*, BSR) [9, 10]. O estudo dos esquemas de proteção e restauração requer também o estudo sobre as heurísticas e algoritmos RSA, já estes são responsáveis pelo estabelecimento dos caminhos de primários e secundários e a alocação dos recursos das demandas de tráfego.

O DLBSPP utiliza o esquema *shared-path protection* (SPP) como base algorítmica incluindo o seu conjunto de restrições, e adicionalmente aplica duas funções heurísticas de custo para computação do caminho primário e do caminho de proteção compartilhado. Assim, é escolhido o caminho que contenha menor carga nos enlaces da rota para o primeiro, e o caminho que contenha menor carga e maior número de compartilhamentos nos enlaces da rota para o segundo. O algoritmo base do SPP proposta em [8] segue a implementação para redes

WDM apresentada em [11]. Porém, nesse trabalho utiliza-se a versão do SPP proposta para EONs em [12], chamada SPP *aggressive sharing policy* (ASP). Juntamente com o DLBSPP foi apresentado um tipo de restauração dinâmica chamada TAR. Nesse tipo de restauração as conexões afetadas por falhas são sequencialmente recuperadas em ordem decrescente de banda requerida.

O esquema seguinte, o BSR, é baseado no contrato de níveis de serviço (*service level agreement,* SLA) que assume que uma conexão cliente pode ter a sua largura de banda reduzida para um mínimo garantido ou recuperada por melhor esforço. O BSR definido nesse trabalho possui três configurações de proteção. A primeira utiliza como base o esquema de proteção de caminho dedicado (*dedicated path protection*, DPP) e aloca para proteção a mesma quantidade de banda requerida. A segunda utiliza a DPP para alocar uma quantidade parcial da banda requerida (redução de banda para proteção). A terceira não se aloca recursos de proteção, porém, utiliza em sua restauração a contração de banda, que reduz a banda requerida até a menor granularidade da grade na tentativa de restaurar o caminho de trabalho (melhor esforço).

A fim de enriquecer a comparação das heurísticas em torno do esquema SPP, propõe-se outra heurística que atua no processo de alocação. A heurística *inverted dual stack* (IDS) foi inspirada na organização interna da memória dos processos. Dentro do espaço de endereçamento do processo possui uma região que é dividia em *heap* e *stack.* A *heap* aloca os ponteiros dos endereços obtidos pela alocação dinâmica e o *stack* empilha as variáveis locais e os ponteiros de retorno das funções. Essas estruturas crescem no sentido de encontro com a outra e eventualmente uma pode ocorrer uma invasão do espaço de endereçamento da outra e causar *overflow*. Na abstração realizada para o IDS, as duas regiões não possuem limites entre si, dessa forma, uma pilha de alocação pode crescer até que atinja a outra extremidade. O objetivo dessa heurística é reservar uma das pilhas de alocação para alocar os caminhos primários e a outra para alocar os caminhos compartilhados, permitindo assim, que a alocação dos recursos compartilhados se concentre em uma região e isso promova o aumento do número de compartilhamentos de slots.

Com o objetivo de aferir o desempenho promovido pelas técnicas de proteção e restauração estudadas, o trabalho visa por meio de um ambiente de simulação programado em linguagem de computador, comparar os esquemas apresentados nos seguintes grupos de comparação: 1) as primitivas DPP e SPP; 2) a restauração dinâmica padrão e o TAR; 3) a proteção obtida pelos de níveis de serviço das conexões em diferentes proporções 4) as variações heurísticas para o SPP apenas por comutação de caminhos e 5) as variações

heurísticas para o SPP com restauração completa. Esta abordagem permite estabelecer a melhor comparação com os esquemas de mesma característica e permite também concluir qual é a melhor solução para determinado tipo de rede e carga de tráfego.

O trabalho é dividido da seguinte forma: o Capítulo 2 apresenta os conceitos relacionados a redes elásticas como a formação do espectro elástico, a arquitetura de nós, o problema de roteamento e alocação de espectro, características básicas do plano de controle e por fim apresenta as principais características da arquitetura EON; o Capítulo 3 explica os esquemas de proteção e restauração, suas classificações de acordo com seu escopo de atuação, assim como os esquemas de proteção DPP e SPP/SPP ASP e de restauração do tipo TAR e BSR; o Capítulo 4 trata dos algoritmos RSA dividindo-os em subproblemas de roteamento e alocação de espectro, além de explicar o funcionamento das heurísticas DLB e IDS referentes aos esquemas dados na seção anterior e que estão incorporados nos algoritmos; o Capítulo 5 define-se a modelagem da simulação utilizada, as métricas e a formulação do problema; o Capítulo 6 apresenta os resultados e as respectivas análises; por último, o Capítulo 7 conclui o trabalho.

2 REDES ÓPTICAS ELÁSTICAS

As redes de comunicações ópticas atuais são baseadas na multiplexação por divisão de comprimento de onda (*wavelength division multiplexing*, WDM) que consiste em combinar vários sinais ópticos, alocados em comprimentos de ondas diferentes, e transmiti-los por uma fibra óptica. As redes WDM exibem desvantagens devido à rigidez de sua grade de frequências e, por isso, foi proposta uma nova arquitetura de rede com grade de espectro flexível: *elastic optical network* (EON). Nesta seção apresentam-se os princípios da formação do espectro elástico em uma EON e sua arquitetura de nós assim como o problema de roteamento e alocação de espetro. Em seguida, explicam-se as funcionalidades do plano de controle e por fim abordam-se brevemente as principais características das EONs.

2.1 O espectro elástico: escalabilidade e flexibilidade

Atualmente a faixa de comprimento de onda de 1260 nm a 1675 nm são mais utilizadas em comunicações ópticas nos sistemas WDM, por isso o *International Telecommunication Union* (ITU) fixou seis bandas espectrais (Figura 1): *Original band* (*O-band* com 1260 nm to 1360 nm), *Extended band* (*E-band* com 1360 nm a 1460 nm), *Short band* (*S-band* com 1460 nm to 1530 nm), *Conventional band* (*C-band* with 1530 nm a 1565 nm), *Long band* (*L-band* com 1565 nm a 1625 nm) e *Ultra long band* (*U-band* com 1625 nm a 1675 nm). A utilização dessas bandas depende do tipo de rede empregada, por exemplo, redes de baixo custo que atendem regiões metropolitanas compreendem da *O-band* à *L-band* com espaçamentos de 20 nm e número reduzido de canais (*Coarse* WDM). Para redes de longas distâncias, a *C-band* e *L-band* são utilizadas por estarem situadas na faixa de ganho de amplificação dos *erbium doped fiber amplifiers* (EDFA). Nessas redes, o espectro é dividido em espaçamentos menores compondo as chamadas *Dense* WDM.

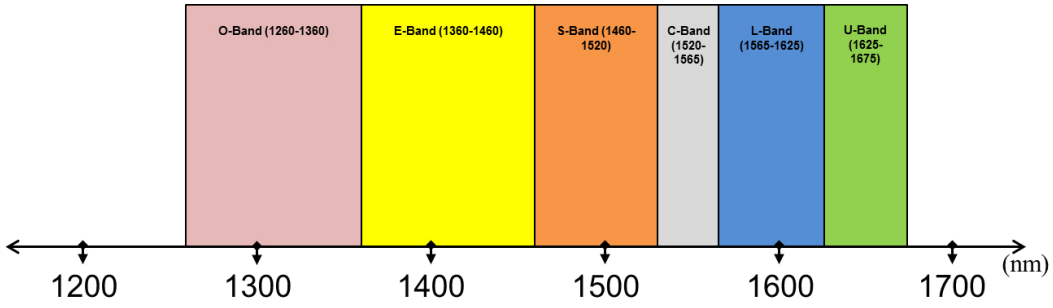


Figura 1 - Definição das bandas do espectro utilizado em comunicações ópticas.

As redes DWDM operam com grade de frequências centrada em 193,1 THz (que corresponde ao comprimento de onda 1552,52 nm) padronizada pelo ITU-T[2]. As frequências dos canais são definidas por $193{,}1 + nS$, em que n é um valor arbitrário inteiro positivo ou negativo incluindo o 0 (zero) e S o valor dos espaçamentos de frequência. O resultado da expressão abrange as bandas C e L do espectro e os espaçamentos de frequências S entre os canais são: 12,5 GHz, 25 GHz, 50 GHz, 100 GHz e múltiplos inteiros de 100 GHz [13]. Por exemplo, em sistemas DWDM com espaçamento de 100 GHz abrangendo a banda C e L permitem alocar mais de 100 canais, sendo 40 canais apenas na banda C.

A principal característica de sistemas (D)WDM é a grade rígida de frequências como mostra a Figura 2. A largura da grade de frequências possui tamanho fixo e são separadas por uma lacuna espectral chamada banda de guarda que impede a sobreposição dos espectros adjacentes, necessária no processo de filtragem e que evita a interferência entre canais na recepção. O tamanho fixo da largura da grade e as bandas de guarda limitam a largura espectral do sinal alocado, não permitindo que o sistema seja flexível em escala e impossibilita, por exemplo, alocar demandas de banda de 400G com formatos de modulação padrão. Outra consequência da utilização desse modelo de grade rígida é o desperdício de banda que ocorre quando uma demanda de conexão de baixa taxa ocupa um comprimento de onda inteiro. Caso o sistema utilize uma grade de 12,5 GHz, o desperdício de banda para demandas de baixas taxas diminuem, mas acentua-se o problema de escalabilidade, pois a largura espectral do canal fica mais limitada. Por outro lado, se utilizada uma grade de 100 GHz ou maior, o sistema torna-se mais flexível em escala, porém, com muito maior desperdício de banda ao alocar demandas de baixas taxas. Portanto, esse modelo de grade não concilia escalabilidade e flexibilidade, o que impede que o espectro seja utilizado eficientemente. Por isso, a utilização de uma grade de espectro flexível e granular das EONs é a solução mais viável atualmente para superar tais problemas [3, 5, 14].

[2] O ITU é dividido em três setores: *Radiocommunication*, *Standardization* e *Development*. O termo ITU-T se refere ao setor *Standardization*.

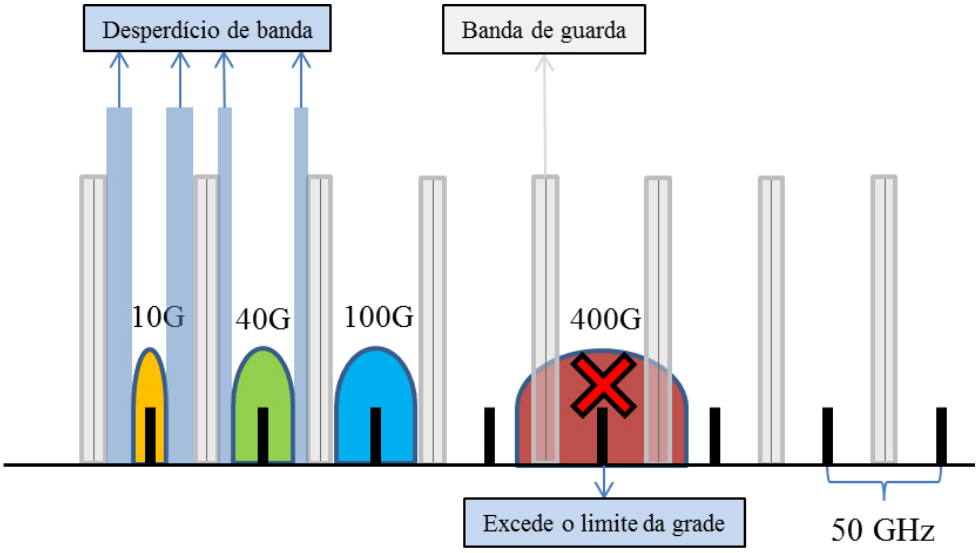


Figura 2 - Alocação de banda em grade rígida de frequências com 50 GHz de espaçamento.

As EONs utilizam tecnologias presentes em redes DWDM de 100G, como formatos de modulação de fase e multiníveis no domínio óptico, multiplexação dos modos de polarização, *lasers* com largura de linha mais estreitas, técnica da detecção coerente e compensação de dispersão no domínio eletrônico com sistemas de processamento digital de sinais (*digital signal processing*, DSP) [3, 14]. Contudo, o salto tecnológico para EONs consiste em obter uma grade espectral com menores espaçamentos e introduzir o conceito de espectro flexível. Por isso, o ITU padronizou um modelo de grade flexível cujas frequências centrais (subportadoras) possuem espaçamentos de 6,25 GHz e largura espectral de 12,5 GHz [13] e espera-se que futuramente sejam padronizadas grades com menores larguras espectrais e espaçamentos. [3, 14].

Dessa forma, uma EON combina dois conceitos na camada óptica: porções espectrais mais estreitas de banda (subportadoras) capaz de alocar uma demanda de conexão a baixas taxas (exemplo: STM-1, STM-4) e a capacidade de agregar subportadoras adjacentes para formar canais de tamanho arbitrários que permitem a formação dos supercanais ópticos. O conceito de supercanal nasceu da ideia de permitir uma capacidade total por canal de 400G ou 1T por maiores distâncias de transmissão com o uso de um conjunto de múltiplas portadoras (*multi-carrier*) muito compactas, com um espaçamento próximo ou igual à taxa de símbolos ao invés da implementação de um formato de modulação em *single-carrier*, cuja tolerância a efeitos de CD e PMD é baixa. Nas EONs do tipo WDM-Nyquist e MB-OFDM, as multiportadoras são geradas, respectivamente, pelas técnicas de filtragem de Nyquist e *optical* OFDM (O-OFDM), que possuem formalismo matemático similar como provado em [15].

A filtragem de Nyquist utiliza pulsos sinc distribuídas no tempo e que formam espectros retangulares com largura de banda próximo ou igual à taxa de símbolos. De forma similar, o O-OFDM utiliza pulsos retangulares no tempo que geram um espectro na forma de um pulso sinc. Essa relação entre Nyquist e O-OFDM é explicado pela propriedade da dualidade da transformada de fourier [16], portanto, a modulação de Nyquist é uma *orthogonal time division multiplexing* (OTDM) [15].

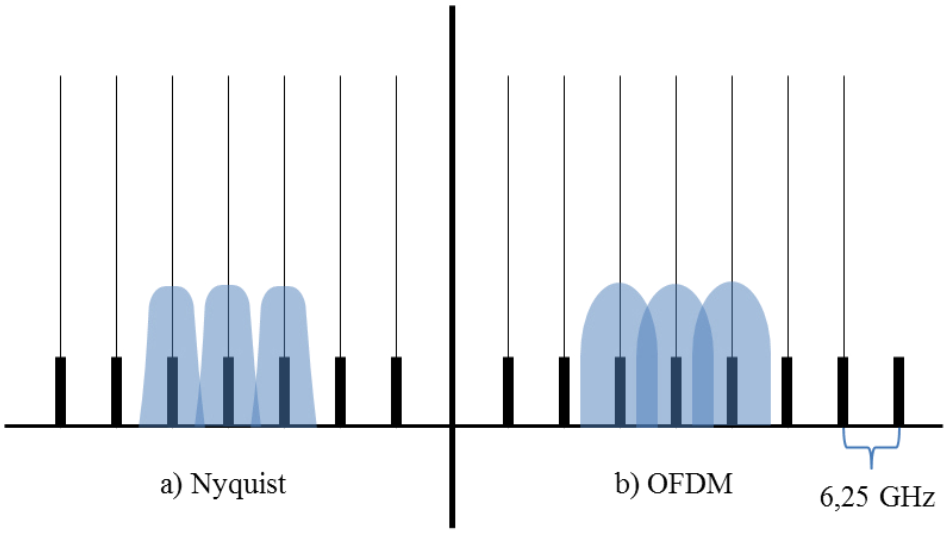


Figura 3 - Grade de espectro flexível. a) Nyquist, b) OFDM.

A grade de espectro granular e flexível padronizada pelo ITU é a abstração do conjunto de subportadoras na camada óptica descritas por suas frequências centrais e larguras de banda. As subportadoras adjacentes geradas pelas técnicas citadas têm parte do seu espectro sobreposto (*overlapping*) formando uma envoltória espectral. Em Nyquist, a sobreposição dos espectros adjacentes ocorre em menor proporção (o pulso retangular teórico não se sobrepõe, mas o pulso real sim) do que no O-OFDM devido ao processo de filtragem. Em ambas as técnicas, a envoltória tem a capacidade de expandir e contrair conforme o número de subportadoras moduladas. Com isso, obtém-se um espectro elástico capaz de acomodar uma demanda de conexão de tamanho arbitrário. A Figura 3 mostra como funciona a agregação na camada óptica nos seguintes casos: na Fig.3a a demanda de conexão é alocada com a técnica de Nyquist com espectro em formato retangular e na Fig.3b uma demanda é modulada por O-OFDM, cujas subportadoras apresentam formas de pulso sinc. O funcionamento dessas técnicas depende da ortogonalidade dos sinais, quer no domínio do tempo (O-OFDM), ou no domínio de frequência (WDM-Nyquist) que permitem que teoricamente um espaçamento mínimo para taxa de símbolo dos canais seja respeitado.

2.2 Arquitetura de nós

A arquitetura de nós de uma rede óptica é formada basicamente por *transponders* (abreviação em inglês de *transmitter-responder*), *optical add-drop multiplexer* (OADM) e *reconfigurable optical add-drop multiplexer* (ROADM). Na arquitetura EON, são apresentados versões sintonizáveis e auto ajustáveis desses dispositivos que habilitam o espectro elástico.

Os *transponders* são equipamentos que possuem os módulos de transmissão (TX), recepção (RX), multiplexadores, demultiplexadores, e controle e monitoramento, como mostra a Figura 4. Eles são responsáveis por transmitir e receber dados convertendo os sinais no domínio eletrônico para o óptico e vice-versa. O módulo TX é composto pela fonte *laser* e o módulo RX corresponde ao fotodetector. Os *transponders* podem ser instalados diretamente nos equipamentos terminais que fazem interface com a rede de dados dos computadores, nos OADM's e nos *optical cross connectors* (OXC's) ou acoplados internamente nos módulos agregados que inserem os canais diretamente nos multiplexadores [17].

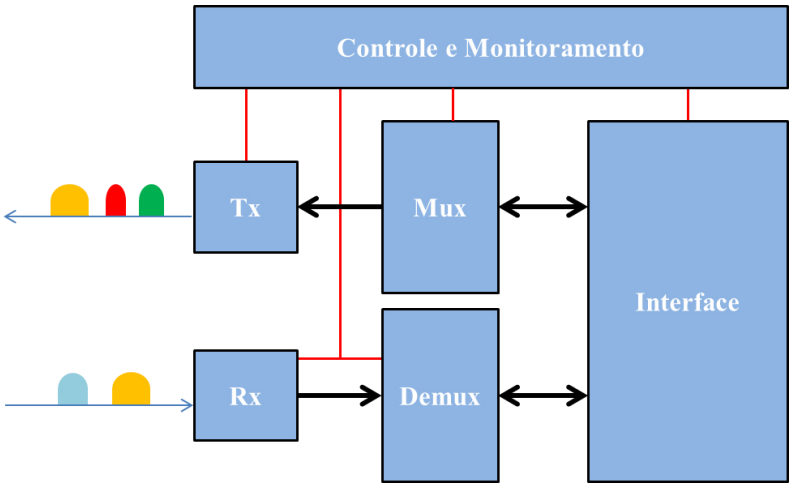


Figura 4 - Diagrama de blocos do *transponder*. Baseado em [18].

Para viabilização da arquitetura de nós EON são necessários dispositivos que ajustam suas janelas espectrais de acordo com o tamanho do espectro a ser alocado no canal. Um modelo de *transponder* que realiza essa função é chamado de *bandwidth variable-transponder* (BV-T). O BV-T tem uma gama de funções adicionais, incluindo o suporte a várias taxas de bits (por exemplo, a partir de 10 Gbs até além de 100 Gbps), mudança dinâmica de formatos de modulação e taxas de símbolos, ajuste do *forward error correction* (FEC) e do formato do espectro óptico. Essa flexibilidade permite ao operador otimizar a

capacidade da rede, configurando o BVT com o formato mais adequado para se obter uma melhor relação de compromisso entre eficiência espectral e distância de transmissão (ver Seção 2.5.2) [19]. Dessa forma, a largura de banda de transmissão (até um valor máximo) é dedicada exclusivamente a uma única demanda de tráfego e um único fluxo de dados é gerado em um único caminho óptico.

Outro modelo de *transponder* flexível mais recente é o *sliceable* BVT (S-BVT) que aprimora as funcionalidades do BV-T por ser capaz de alocar a banda em um ou mais fluxos ópticos independentes, que são transmitidos para um ou mais caminhos ópticos. Ao contrário dos BV-Ts, a sua largura de banda de transmissão pode ser dividida para servir várias demandas de tráfego independentes simultaneamente. No exemplo da Figura 5 é mostrado como funciona esse processo. No primeiro caso, a demanda de 1T é transmitida em dois fluxos de dados, um contendo 6 subportadoras e outro contendo 4, que são associados a caminhos ópticos diferentes. O mesmo ocorre para a demanda de 200G e somente a demanda de 100G associa um fluxo dedicado a um único caminho óptico como ocorre no BV-T tradicional. Além disso, é possível também programar o formato de modulação de cada subportadoras individualmente [19].

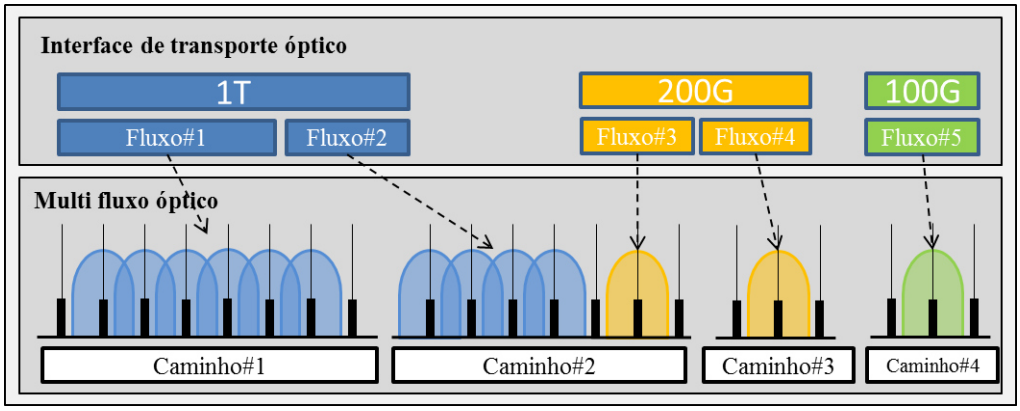


Figura 5 - Associação entre fluxos de dados e caminhos ópticos em um S-BVT. Adaptado de [19].

Nas redes WDM, os equipamentos (OADM) atuam na comutação do comprimento de onda, que efetuam a multiplexação e demultiplexação de comprimentos de onda e permitem sua passagem (*pass through*) para as interfaces de saída, por exemplo, *transponders* ou fibras. O OADM utiliza *lasers* e filtros fixos para comprimentos de onda fixos que os adicionam ou removem em um ponto do nó. Dessa maneira, o OADM funciona com comutação fixa, de maneira pré-configurada, por isso não permite flexibilidade para variações de demanda de banda, uma vez que as configurações devem ser efetuadas manualmente.

Uma versão mais versátil do OADM é o ROADM, que adiciona e remove os comprimentos de onda em um ponto do nó remotamente em vez de exigir a presença de um técnico para configurar lasers e filtros específicos do sistema. Os ROADMs permitem que os sistemas usem comutação óptica dinâmica e isso evita a conversão *optical-eletro-optical* (OEO) desnecessária, que traz vantagens significativas para as operadoras e os provedores de serviços, uma vez que a implantação de dispositivos de comutação no domínio eletrônico envolve maiores custos de implantação e aumenta o consumo de energia dos equipamentos. Dessa forma, o número menor de elementos de rede reduz as despesas operacionais e aumenta a confiabilidade do sistema. Além disso, os ROADMs reduzem a complexidade na gerência de tráfego, pois os comutadores ópticos são transparentes ao formato de modulação e à taxa de transmissão dos canais. Um equipamento semelhante ao ROADM, chamado *add drop regenerators* (ADR), pode ser utilizado para regeneração OEO do sinal efetuando as operações de *add* e *drop* em um mesmo comprimento de onda [20].

Normalmente um ROADM é caracterizado pelo número de graus, ou direções, de comutação que pode executar. A primeira geração de ROADMs só podia comutar comprimentos de onda em dois graus, geralmente chamado de "*East*" e "*West*". A segunda geração de ROADMs podia comutar em quatro graus ("*North*", "*South*", "*East*" e "*West*") [21]. A terceira e mais moderna geração de ROADMs permite grau de ordem N e podem ser construídos com dois tipos de componentes: *optical cross-connect* (OXC) e *wavelength selective switch* (WSS). A Figura 6 mostra um ROADM construído com OXCs em que os sinais de cada interface de entrada são demultiplexados e direcionados para os OXCs, que por sua vez comutam os comprimentos de onda para as interfaces de saída.

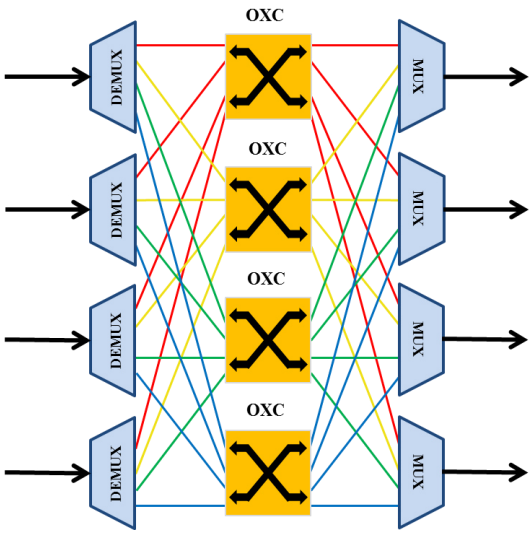


Figura 6 - ROADM construído com OXC [22].

A Figura 7 apresenta o funcionamento do WSS. Um WSS é uma matriz de comutação formada por elementos dispersivos que demultiplexam o feixe óptico e elementos de comutação que direcionam os comprimentos de onda para portas separadas. Assim o componente é capaz de selecionar o(s) comprimento(s) de onda para determinada porta.

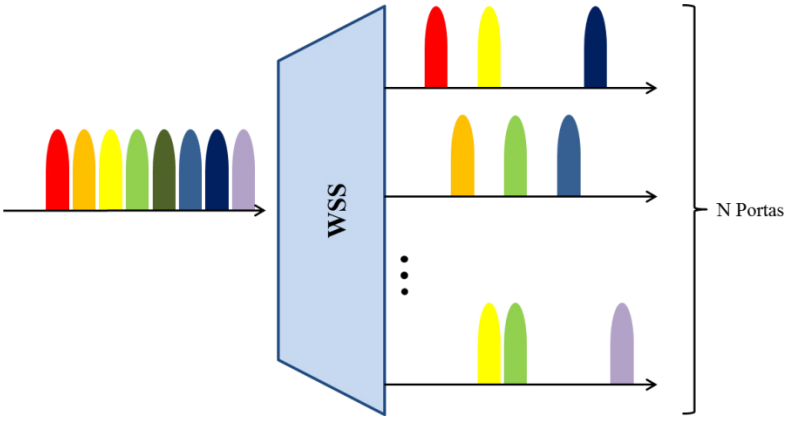


Figura 7 - Funcionamento do WSS [22].

A arquitetura EON conta com o ROADM flexível cujo componente chave é *bandwidth variable-wavelength selective switch* (BV-WSS). O dispositivo BV-WSS configura a largura de banda óptica passante da janela de roteamento de acordo com a largura espectral do sinal óptico de entrada. Um BV-WSS pode ser construído com base em *micro-electro-mechanical systems* (MEMS) e *liquid crystal on silicon* (LCoS), que são os principais elementos de comutação [23].

2.3 O problema de roteamento e alocação de espectro

O processo de estabelecer uma conexão fim a fim na camada óptica de uma rede (D)WDM é semelhante ao de uma rede de comutação de circuitos. Para isso é preciso alocar um caminho óptico, ou seja, um comprimento de onda livre em todos os enlaces da rota. Em uma rede óptica transparente, um caminho óptico é formado pelo mesmo comprimento de onda em todos os nós da rota. Nos nós em que os roteadores são equipados com conversores de comprimento de onda é possível que o caminho óptico seja atribuído a outro comprimento de onda e, assim, o fator limitante no estabelecimento da conexão é o número de comprimentos de onda livres em cada nó. Como a disponibilidade desses conversores é limitada, então o estabelecimento do caminho óptico obedece à restrição de continuidade de comprimento de onda.

O problema de encontrar caminhos e atribuir comprimentos de onda para um caminho óptico é chamado de *routing and wavelength assignment* (RWA). Algoritmos RWA são aqueles que resolvem esse tipo de problema, que geralmente é encontrar o caminho mais curto, que contenha comprimentos de onda livres para serem atribuídos e que garantam a restrição de continuidade de comprimento de onda ao longo dos enlaces da rede. Esse tipo de problema tem complexidade NP-completo (*nondeterministic polynomial time*, NP), pois não existem algoritmos que possam encontrar a uma solução ótima em tempo polinomial [24]. Quando o problema RWA é tratado em conjunto, ou seja, quando o algoritmo encontra um caminho e um comprimento de onda ao mesmo tempo, o número de variáveis tende a aumentar rapidamente com o aumento do tamanho da rede. Uma maneira de simplificar a solução do problema RWA é tratá-lo separadamente em um subproblema de roteamento e outro de atribuição de comprimento de onda. Apesar desta separação não garantir uma solução ótima, proporciona uma redução no tempo de computação.

Semelhante ao problema RWA em redes WDM, nas EONs o problema passa a ser de roteamento e alocação de espectro (*routing and spectrum allocation*, RSA). Enquanto o caminho óptico em um problema RWA consiste em encontrar um comprimento de onda, em um problema RSA trata-se de encontrar uma porção de espectro de tamanho suficiente para atender a demanda de tráfego. O problema RSA é mais desafiador do que o RWA porque necessita atender duas restrições: 1) o espectro deve ser contínuo em todos os enlaces da rota e 2) a porção espectral formada não pode ter lacunas, ou seja, a porção espectral forma uma envoltória contínua (contiguidade). A restrição 2 é resultado direto das técnicas de geração *multi-carrier* apresentadas na Seção 2.1, mas é preciso que essa restrição seja explicitamente testada pelos algoritmos RSA, averiguando-se o conjunto adjacente de subportadoras que forma a porção de espetro desejada [6]. Além disso, para evitar interferência entre os canais na recepção é preciso que os caminhos ópticos que compartilham um enlace sejam alocados com uma banda de guarda entre eles. Nesse caso, os algoritmos RSA são responsáveis por posicionar adequadamente a banda de guarda entre os canais formados.

O problema RSA compreende tanto o problema de encontrar caminhos em uma rede quanto de alocar os recursos espectrais. Um problema desse tipo possui mais de uma solução e geralmente é um problema de otimização ao invés de apenas um problema de decisão, ou seja, busca-se sempre a melhor solução entre todas as soluções factíveis de acordo com algum critério. Um algoritmo que encontra uma solução otimizada conjunta para o problema RSA tem complexidade NP-difícil e em redes de grande dimensão o problema não é tratável com programação linear. Por esse motivo, geralmente o problema é tratado separadamente em um

subproblema de roteamento e outro de alocação de espectro e heurísticas são utilizadas para se obter uma solução aceitável que, mesmo não garantindo uma solução ótima, seja uma solução próxima da ótima, mas com um tempo de computação muito menor. O problema tratado separadamente e com a utilização de heurísticas tem complexidade NP-completo e a solução pode ser verificada em tempo polinomial [6].

Em uma rede em que as demandas de tráfego são previamente determinadas (rotas conhecidas), o problema RSA passa a ser um problema de alocação estática de espectro. Em redes com demanda dinâmica de tráfego, os algoritmos RSA precisam constantemente encontrar as rotas e alocar o espectro de acordo com a situação da rede naquele instante de conexão. Em ambos os casos, se a capacidade da rede for excedida ou as restrições não forem validadas, a conexão de entrada é bloqueada. O percentual de conexões bloqueadas em relação ao total de conexões de entrada é chamado de taxa de bloqueio e é a principal métrica utilizada para medir a eficiência de um algoritmo RSA (ver Seção 5.2). A Seção 4 irá tratar desses algoritmos RSA com mais detalhes.

2.4 Plano de Controle

As redes de telecomunicações são tradicionalmente divididas em três níveis de abstração: plano de dados, plano de controle e plano de gerenciamento. O plano de dados, também conhecido como *forwarding plane*, é responsável por encaminhar o tráfego do cliente para o próximo roteador no caminho de rede selecionado de acordo com a lógica do plano de controle. O plano de controle é responsável pela descoberta da rede e por tomar decisões quanto ao estabelecimento e manutenção do tráfego. O plano de gerenciamento é o que transporta o tráfego administrativo da rede que permite o operador de rede acessar e configurar os dispositivos, por exemplo, configurar subredes, definir as tabelas de roteamento estático, e monitorar as suas operações [25]. Em uma rede convencional, todos os três planos são implementados no firmware dos roteadores e comutadores. Na abordagem de redes definidas por software (*software defined network*, SDN), o plano de controle é desacoplado do plano de dados e implementado em software. O SDN permite gerenciar serviços de rede por meio da abstração das funcionalidades de nível mais baixo utilizando programação de alto nível, proporcionando flexibilidade e agilidade para atender as necessidades específicas de uma rede.

Um plano de controle compreende um conjunto de protocolos responsáveis por rastrear a topologia e o estado dos recursos da rede, e por estabelecer, remover e manter as

conexões, entre outras características como: agregação de tráfego, QoS, e as estratégias de sobrevivência. A evolução dos planos de controle projetados e padronizados para redes WDM ainda está em um estágio inicial para abranger a tecnologia EON. Para isso, é preciso satisfazer alguns requisitos principais como:

1) Permitir que os canais ópticos sejam flexíveis em tamanho e largura;
2) Permitir que os canais ópticos suportem vários formatos de modulação e modos de polarização;
3) Permitir o redimensionamento de canal;
4) Seguir as definições de frequências flexíveis padronizadas pelo ITU em [13];
5) Habilitar supercanais a serem alocados em uma parte contígua do espectro;
6) Suportar roteamento orientado a conteúdo em porções de espectro que compõe um supercanal;
7) Ser capaz de gerenciar os nós que têm funcionalidades de grade rígida ou grade flexível, permitindo a implantação de segmentos de grade flexível em uma rede de grade fixa;
8) Permitir restauração rápida na ocorrência de falhas, com ou sem caminhos pré-reservados;
9) Habilitar a restauração reversível, restabelecendo a rede para o estado original, uma vez que a falha seja corrigida.

Segundo [26], os principais planos de controle em desenvolvimento para EONS são:

- *Generalized multiprotocol label switching* (GMPLS): é uma extensão do *multiprotocol label switching* (MPLS) usada nas redes comutadas por pacotes e adaptada para redes ópticas. O GMPLS é a solução de plano de controle atual em redes convencionais WDM e é comporto por três principais protocolos: *resource reservation protocol with traffic engineering* (RSVP-TE), *open shortest path first with traffic engineering* (OSPF-TE) e *link management protocol* (LMP);
- *OpenFlow*: é um protocolo aberto que permite a separação de dados e plano de controle (arquitetura SDN). Esse protocolo é baseado em fluxo de comutação com a capacidade de executar aplicações de roteamento, controle e gestão definidos por software em um controlador *OpenFlow* centralizado.

- *Path Computation Element* (PCE): é uma solução independente que simplifica a computação de caminhos e recursos separando a determinação topologia de rede da criação de caminho. O PCE é aplicado tradicionalmente em roteadores *head-end* que suportam *interior gateway protocol* (IGP) dentro do seu domínio e *border gateway protocol* (BGP) entre domínios. A arquitetura PCE suporta os modelos de computação de caminho centralizado e distribuído. No modelo centralizado há um único PCE que processa todas as solicitações de caminho. Uma vez que este modelo tem um ponto único de falha, um PCE backup pode assumir a responsabilidade de computação em caso de falha do PCE principal. No modelo de computação distribuída, vários PCEs podem ser implantados operando independente ou por diferentes PCEs coordenados.

As funcionalidades do plano de controle são alcançadas principalmente por meio de dois mecanismos: protocolo de roteamento e protocolo de sinalização como mostra a Figura 8. A seguir apresenta-se o propósito geral dos protocolos de roteamento e de sinalização.

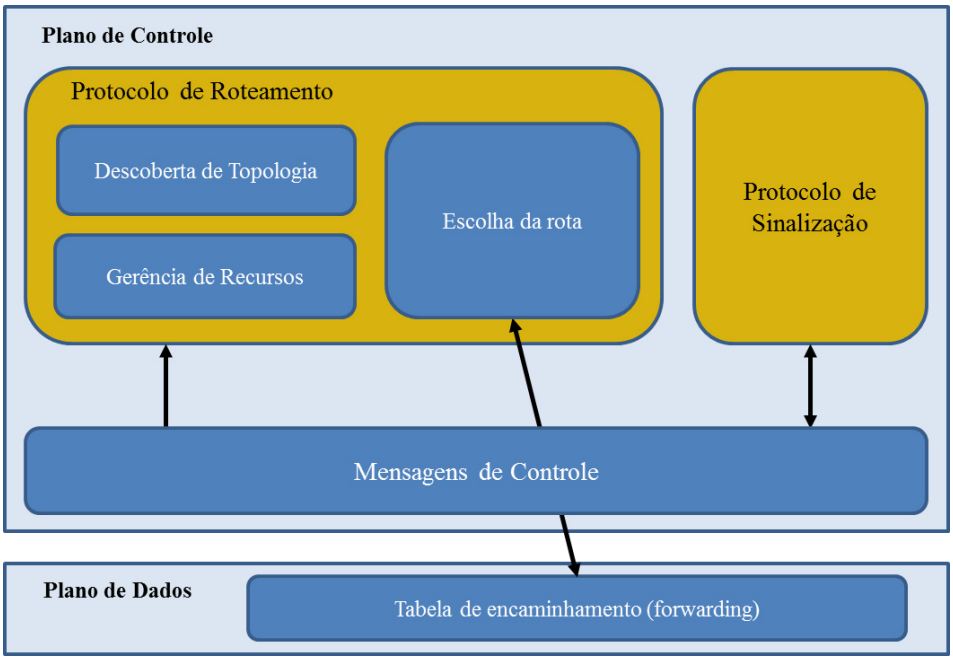


Figura 8 - Diagrama de funcionalidades do plano de controle.

2.4.1 Protocolo de Roteamento

O protocolo de roteamento é responsável pela divulgação de informações de forma confiável sobre o estado da topologia e dos recursos (por exemplo, largura de banda disponível) dentro e entre domínios de roteamento da rede. Essas informações são transmitidas por mensagens de controle pelo canal de controle da rede. As mensagens de controle são essenciais para as tomadas de decisão dos protocolos de roteamento, pois em uma rede dinâmica, enlaces e/ou nós podem falhar e cada mudança de estado requer o recálculo das rotas e, assim, é preciso que o protocolo de roteamento tome conhecimento da topologia alterada da rede e do estado de seus recursos. Para que o protocolo de roteamento seja escalável é importante selecionar cuidadosamente quais informações serão anunciadas, pois trocas excessivas de mensagens de controle podem resultar em falhas no protocolo.

Ao contrário das redes de comutação de pacotes, as redes ópticas (comutação de circuito) gerenciam explicitamente os recursos de rede (largura de banda) para cada conexão. Como resultado, os protocolos de roteamento são estendidos para permitir a distribuição de informações de recursos dos enlaces da rede [27]. Nas redes EONs, o protocolo de roteamento lida com o problema RSA (Seção 2.3) que envolve o reconhecimento da topologia de rede e do estado dos *slots* de frequência dos enlaces da rede. Em seguida, o roteamento é resolvido por meio dos algoritmos RSA, que pode ser realizado off-line, durante a fase de planejamento, ou on-line em um cenário dinâmico. Ele pode ainda ser realizado por uma entidade centralizada, como o PCE ou distribuído por todo elementos de rede como na arquitetura GMPLS [26]. Por fim, o plano de controle configura a tabela de encaminhamento no plano de dados ao longo da rota obtida (Figura 8), utilizando do protocolo de sinalização.

2.4.2 Protocolo de Sinalização

O protocolo de sinalização serve para anunciar a mudança de estado das conexões de rede além de lidar com a perda de mensagens, erros de execução nos nós da rota e falhas do módulo de sinalização As principais sinalizações de mudança de estado das conexões são: criação, manutenção, restauração e exclusão.

Como vimos na seção anterior, o protocolo de roteamento é responsável por encontrar a rota e os recursos necessários que atenda uma demanda de conexão. No momento da criação da conexão o protocolo de sinalização envia mensagens para os roteadores da rota e configuram a reserva desses recursos. Depois de estabelecida, o protocolo de sinalização tem

a função de manter atualizado o estado da conexão que pode utilizar uma das duas principais abordagens: *soft-state* e *hard-state*. Na abordagem *soft-state* uma mensagem de atualização temporizada é sincronizada entre o remetente e o receptor da sinalização. O estado da conexão se mantém enquanto as mensagens de atualização estiverem sendo recebidas antes de esgotar o tempo do temporizador. Nessa abordagem, perdas de mensagens podem causar uma falsa remoção de estado. Por esse motivo, as conexões em redes ópticas utilizam a abordagem *hard-state*, em que a detecção de sinalização do emissor e do receptor é confiada a um sinal externo com mecanismos para detectar e lidar com falhas no módulo de sinalização e no canal de controle, assim seus estados são normalmente finalizados [28].

Uma conexão ativa pode ter duas mudanças de estado: 1) a conexão pode ser interrompida por uma falha ocorrida nos enlaces da rede ou nos componentes presentes nos nós ou 2) a conexão pode ser finalizada pelo usuário. No primeiro caso, em redes tolerantes a falhas existem mecanismos de proteção e restauração que garantem a sobrevivência das conexões interrompidas. Normalmente, uma conexão do usuário utiliza dois caminhos disjuntos no plano de dados: um para atender os serviços e outro para restaurá-la. O tráfego de dados pode ser encaminhado para um caminho, enquanto o outro caminho é utilizado apenas caso o primeiro falhe. Este modelo de restauração é viável em redes orientadas a pacotes, porque os caminhos de proteção não consomem largura de banda se nenhum dado for transmitido. Em redes ópticas, no entanto, um caminho de proteção consome largura de banda independentemente se os dados são enviados. Alguns esquemas de restauração mais rápidos requerem que sejam estabelecidos caminhos de proteção com antecedência, ou seja, no momento do estabelecimento da conexão. Sejam esses esquemas de proteção baseados em enlace ou caminho (ver Seção 3.1.1 e Seção 3.1.2), geralmente eles utilizam uma grande quantidade de recursos da rede. Uma maneira de reduzir a utilização de recursos para proteção é compartilhar a largura de banda com outros caminhos de trabalho (Seção 3.3). Estes esquemas introduzem diferentes relações de compromissos entre o tempo de recuperação da conexão e a taxa de utilização de recursos de rede. Quando a conexão não dispõe de pré-reserva de recursos, os algoritmos RSA podem ser executados novamente para reestabelecer a conexão em tempo real. Assim, o protocolo de sinalização é necessário para sinalizar o processo de restauração das conexões afetadas por falhas, seja pelo acionamento da proteção ou pela restauração dinâmica. A restauração de uma conexão é iniciada a partir de gatilhos que são obtidos dos hardwares que monitoram os canais ópticos. O equipamento que realiza essa função é o *optical performance monitor* (OPM), que tem como principais funções medir a potência e a relação sinal ruído óptico de cada canal [29]. O OPM possui outros elementos

de monitoramento que medem, por exemplo, o formato do pulso, dispersão cromática e dispersão dos estados de polarização do sinal. Portanto, uma rede mal configurada pode disparar esses gatilhos e emitir falsos alertas de falha.

Por último, a sinalização de exclusão de conexão que corresponde ao segundo caso é iniciada quando o usuário emite explicitamente o comando de término da conexão. As operações de restauração e exclusão precisam ser bem coordenadas pelo plano de controle, uma vez que um desligamento de sinal em um nó antes da notificação de exclusão de conexão pode ser confundido com uma falha pelo nó final e este iniciar o processo de restauração antes da exclusão da conexão. É por isso que uma das técnicas utilizadas para a exclusão da conexão é efetuar a sinalização em duas fases. A primeira fase de sinalização (a partir do nó de origem do pedido de exclusão para o nó destino) informa os nós da intenção de eliminar a conexão e desativa a detecção de alarme de monitoramento para o canal da conexão em exclusão. Então, depois é executada em ordem reversa a remoção da conectividade e a liberação dos recursos. O procedimento de sinalização de duas fases para a exclusão de conexão também é importante para assegurar que as conexões são totalmente excluídas. Conexões parcialmente excluídas consomem recursos de rede e gera um custo significativo para o operador de rede.

2.5 Características principais do EON

Nesta seção, descrevem-se algumas das principais características das EONs, como: eficiência espectral, distância adaptativa, economia de energia e fragmentação do espectro.

2.5.1 Eficiência espectral

Uma das maneiras de aumentar a taxa total de transmissão em meio óptico é aumentar a eficiência espectral ao escolher formatos de modulação multiníveis de mais alta ordem [30, 31]. A modulação é o processo pelo qual a informação é transmitida variando os parâmetros de amplitude, frequência, fase, polarização de uma onda portadora. Os bits de informação são codificados através de símbolos. Quanto maior a quantidade de símbolos, maior a quantidade de bits por símbolo transmitido para uma mesma taxa de bits. Assim os formatos de modulação multiníveis reduzem a taxa de símbolos possibilitando maior robustez às distorções do sinal oriundas de efeitos dispersivos, como a CD ou PMD. Por outro lado, os formatos de modulações de mais alta ordem são menos tolerantes aos efeitos não lineares da

fibra, como os ruídos de fase, devido à distância reduzida entre os símbolos, portanto o alcance de transmissão óptica é reduzido [32].

No entanto, alterar o formato de modulação não é a única solução para aumentar a eficiência espectral total em redes de 400G/1T por canal. Como explicado na Seção 2.1, a grade rígida de frequência causa desperdício de banda nos casos em que a demanda de banda alocada ocupa um espectro menor que a grade do sistema. É por isso que para obter mais eficiência espectral total é preciso também considerar essas porções de espectro que ficam inutilizados. O aproveitamento dessas porções espectrais é possível devido à grade flexível das EONs que permite acomodar melhor as demandas de tráfego, como mostra a Figura 9. Na Fig.9a, duas demandas, uma de 100 Gbps e outra de 40 Gbps em uma grade fixa que é separada pela banda de guarda. Na Fig.9b, as mesmas demandas são alocadas uma rente à outra em uma grade flexível e a banda de guarda é alocada entre elas. Esse tipo de alocação aproveita melhor o espectro e reduz os recursos espectrais necessários para alocar as demandas de tráfego [14].

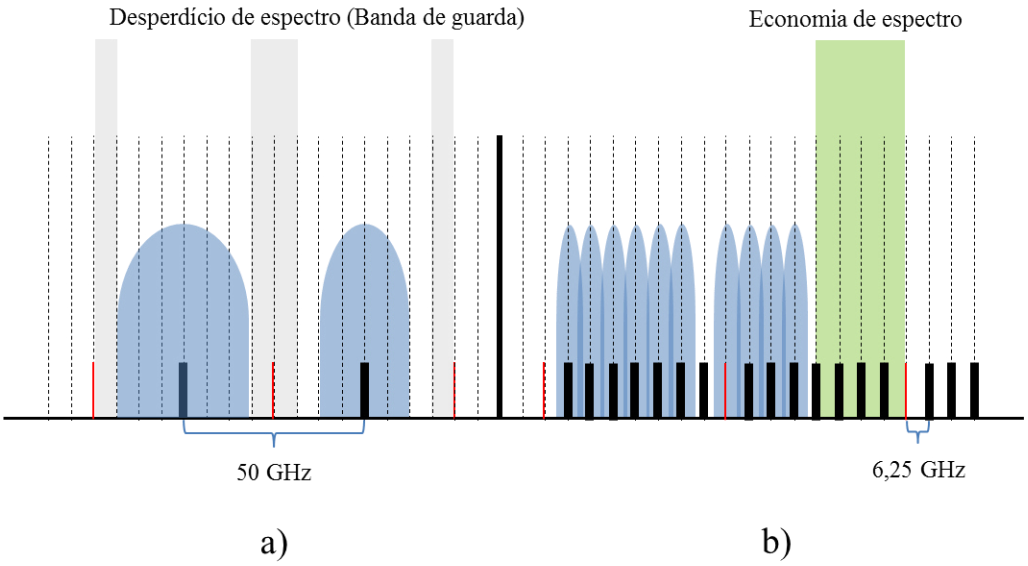


Figura 9 – Comparação da alocação de banda. a) Grade fixa que mantém as bandas de guarda entre os caminhos ópticos que transmite duas demandas, uma de 100 Gbps e outra de 40 em uma grade rígida de frequências; b) os canais das demandas podem ser alocados em um espectro flexível provendo uma economia de 4 slots de frequência de espectro. Baseado em [14].

2.5.2 Distância adaptativa

Os formatos de modulação de mais alta ordem aumentam a eficiência espectral e provê robustez ao sinal contra os efeitos de CD e PDM. Por outro lado, a maior proximidade

entre os símbolos do sinal são mais suscetíveis a distorções provocados por efeitos não lineares da fibra. Essas distorções diminuem o alcance de transmissão e exige uma maior relação sinal ruído no receptor. Por esse motivo, a escolha do formato de modulação deve considerar a qualidade da transmissão (QoT) que é medida pela taxa de erro de bit na recepção para uma distância de transmissão desejada. A Tabela 3 apresenta a ordem de alguns formatos de modulação e a Figura 10 apresenta a relação de compromisso entre o nível de modulação e a distância de transmissão para um QoT aceitável [5].

Tabela 3 - Formatos de modulação

Formato de Modulação	**Símbolos da constelação**
BPSK	2
QPSK	4
8-QAM	8
16-QAM	16

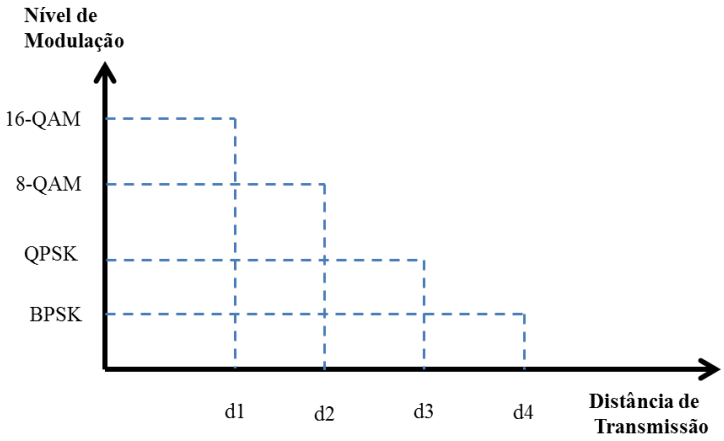


Figura 10 - Nível de modulação e distância de transmissão para QoT aceitável. Adaptado de [5].

As EONs, compostas de *transponders* de banda variável (Seção 2.2) permitem a utilização de diferentes formatos de modulação para cada demanda de tráfego. Dessa forma, o plano de controle pode selecionar um formato de modulação que atenda a essa relação de compromisso representada na Figura 10. Essa característica chama-se distância adaptativa.

Um exemplo do funcionamento da distância adaptativa é apresentado na Figura 11. Nesse exemplo, dois tráfegos 400 G são transmitidos por distâncias diferentes, sendo a primeira de 1400 km e a segunda de 200 km. Dessa forma, o plano de controle seleciona o formato de modulação adequado para cada transmissão com a finalidade de economizar espectro e obter uma QoT aceitável no receptor. O formato de modulação escolhido para

transmitir por 1400 km (Fig.11a) é de ordem menor do que o formato que transmite em 200 km (Fig.11b), segundo os dados da Tabela 3, resulta em um espectro mais largo. Um terceiro tráfego de 100 G percorre 400 km (Fig.11c) e o formato de modulação escolhido é de ordem intermediária que satisfaz o QoT.

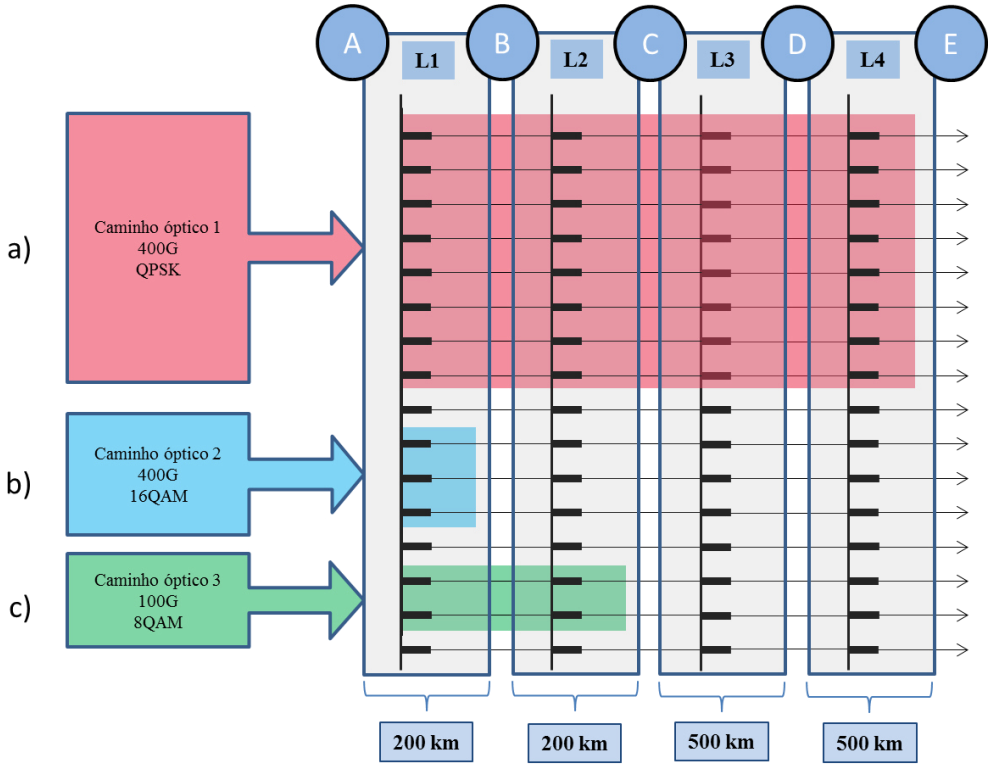


Figura 11 – Representação de uma rede (nós A-B-C-D-E, enlaces L1, L2, L3, L4). São alocados três caminhos ópticos que atendem a três demandas de conexão. a) O tráfego de 400G alocado no caminho óptico 1 percorre uma distância de 1400 km e, neste caso, diminui-se a ordem do formato de modulação, b) outro tráfego de 400G alocado no caminho óptico 2 percorre uma curta distância (200 km) que permite a utilização de um formato de modulação de mais alta ordem, e c) o tráfego de 100G alocado no caminho óptico 3 percorre uma distância intermediária (400 km), portanto um formato de modulação intermediário é selecionado.

2.5.3 Gerenciamento eficiente de energia

Outra característica da arquitetura EON é que permite o gerenciamento eficiente de energia da rede. Podem-se observar benefícios significativos em termos de eficiência de energia para redes com tamanhos diferentes e para diferentes condições de tráfego graças aos formatos de modulação adaptativa e à granularidade fina da grade flexível.

O benefício da granularidade fina permite uma melhor adaptação do recurso espectral alocado à demanda de tráfego, enquanto que a modulação adaptativa introduz a flexibilidade

de selecionar o formato de modulação mais adequado de acordo com a demanda e a distância de transmissão, minimizando assim o número de regeneradores na rede. Além disso, em uma EON com baixa demanda de tráfego é possível desativar alguns *transponders* para evitar o consumo desnecessário de energia [3]. Por outro lado, em uma EON com alta demanda de tráfego, a sua eficiência espectral tem um impacto direto na taxa de bloqueio de rede. Desta forma, a taxa de bloqueio mais baixa oferecida pela rede permite lidar com volumes maiores de tráfego e evitar a implantação de elementos de rede adicionais, que não só implica um custo mais elevado, como também um aumento do consumo de energia total da rede [33].

2.5.4 Fragmentação do Espectro

Um dos desafios que ainda precisam ser superados em relação à arquitetura EON é a fragmentação do espectro. A fragmentação espectral como mostrado na Figura 12 é decorrente do processo de alocação de banda que resulta em lacunas espectrais sem utilização, principalmente em cenário dinâmico de tráfego [3]. A Fig.12a mostra o estado inicial de utilização do espectro em que são alocadas demandas de tráfego de vários tamanhos e separadas por bandas de guarda. Na Fig.12b, uma conexão é liberada deixando livre um recurso espectral que é menor do que o recurso espectral necessário para alocar a nova demanda (note que dois slots devem ser reservados para as bandas de guarda), mostrada na Fig.12c. Dessa forma, a nova conexão será alocada em outra parte do espectro, gerando lacunas espectrais. Outra conexão é liberada (ver Fig.12d) e, dessa vez, resulta em duas lacunas espectrais insuficientes para alocar uma nova demanda (ver Fig.12e) e, como não há nenhum outro recurso disponível, ocorre bloqueio de conexão.

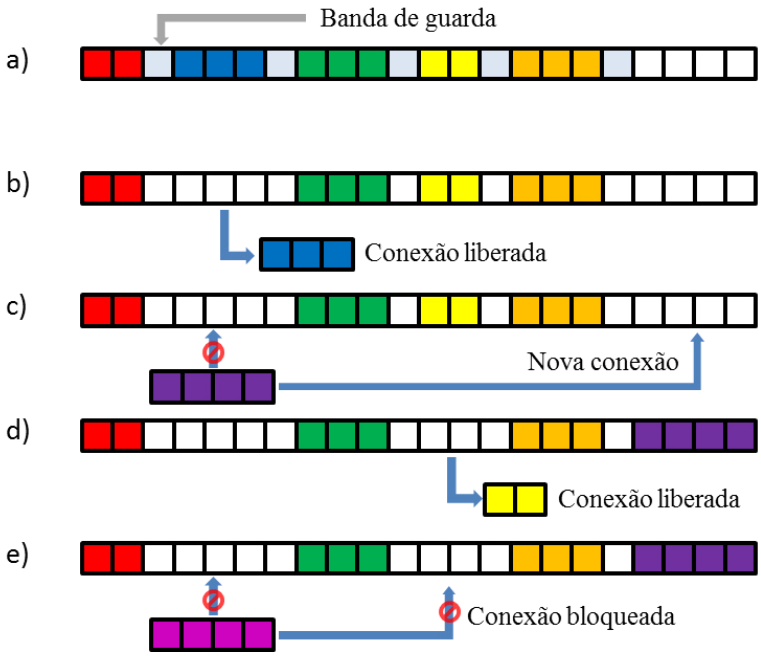


Figura 12 - Fragmentação do espectro: a) espectro ocupado; b) espectro central liberado; c) alocação de um novo espectro não encaixa na lacuna formada, realocada em outra faixa espectral (lacuna inutilizada); d) outro espectro é liberado; e) a conexão não se encaixa em nenhuma das duas lacunas deixadas e é bloqueada.

3 ESQUEMAS DE PROTEÇÃO E RESTAURAÇÃO

A sobrevivência é a capacidade que a rede tem de garantir o funcionamento das conexões mesmo sob a ocorrência de falhas que podem ser em nós ou em enlaces. O gerenciamento de falhas tem se tornado um problema crítico para sobrevivência de redes ópticas que operam em taxas de bit elevadas, devido ao grande volume de tráfego transportado. Uma falha em um nó ou enlace da rede pode acarretar a perda de grande volume de dados e a interrupção de múltiplos canais de serviços. Portando, garantir a sobrevivência significa torná-la tolerantes a falhas e, por isso, a rede deve dispor de esquemas de proteção e/ou restauração.

A proteção de rede consiste em reservar recursos para uso dedicado na transmissão do tráfego afetado por uma falha na rede. A proteção é um mecanismo proativo, pois os recursos são reservados no momento do estabelecimento da conexão, antes da ocorrência de qualquer falha. Por isso, quando uma conexão está assegurada por um esquema de proteção ela tem uma recuperação rápida e mais garantida em caso de falha.

A restauração de rede é o processo de rearranjar as rotas através dos recursos disponíveis distribuídos por toda a rede. No mecanismo de restauração de rede não é realizada a reserva prévia de recursos; estes são alocados após a ocorrência e detecção da falha e, por isso, é chamado de mecanismo reativo. Em um esquema de restauração de rede, a recuperação da conexão não é garantida, pois depende dos recursos disponíveis na rede no momento da ocorrência da falha; e o seu tempo de reestabelecimento da conexão é mais longo que nos esquemas de proteção devido ao processo de recalcular a nova rota e os recursos necessários.

A seguir, são descritos esquemas de proteção e restauração incluindo os que são objetos deste estudo, a saber: proteção de caminho dedicado (*dedicated path protection*, DPP) [34], proteção de caminho compartilhado (*shared path protection*, SPP) [12], restauração ciente do tráfego (*traffic-aware restoration*, TAR) [8] e restauração por contração de banda (*bandwidth squeezing restoration*, BSR) [10].

3.1 Classificação dos esquemas

Os esquemas de proteção e restauração são classificados de acordo com sua atuação (ver Figura 13): no enlace, caminho ou subcaminho. Os exemplos apresentados a seguir são aplicados a uma rede em malha de 8 nós.

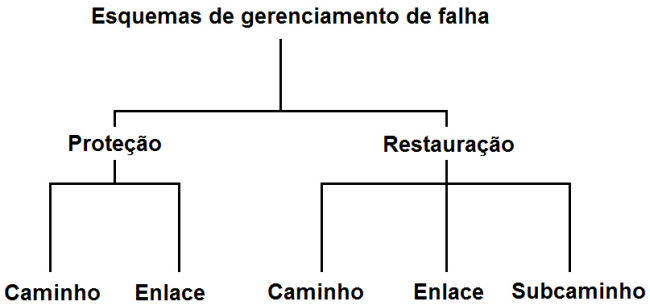


Figura 13 - Classificação dos esquemas de gerenciamento de falha, adaptado de [35]

3.1.1 Atuação em enlace

Quando ocorre uma falha em um enlace, nos esquemas de proteção e restauração baseados em enlace os nós das extremidades deste enlace sinalizam o encaminhamento das conexões afetadas em torno do enlace da falha, isto é, os nós que participam da falha continuam fazendo parte do caminho das conexões e caminhos intermediários são definidos a partir deles.

A Figura 14 mostra como funciona a recuperação de uma conexão cliente com um esquema de proteção baseado em enlace. Na Fig.14a há uma fibra de proteção e quando uma falha ocorre no enlace entre os nós 1 e 2, as conexões são encaminhadas pelo enlace de proteção em torno dos mesmos nós, como mostra na Fig.14b.

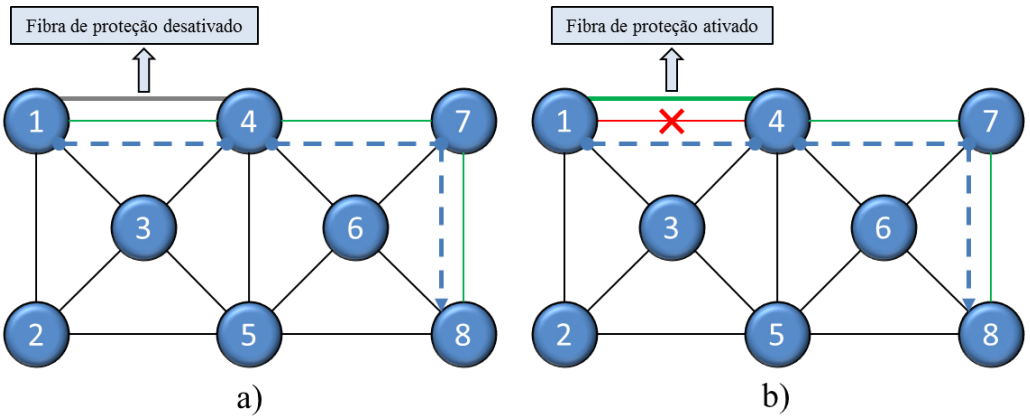


Figura 14 – Proteção baseada em enlace: a) um enlace de proteção dá suporte ao enlace entre os nós 1 e 2; e b) uma falha no enlace entre os nós 1 e 2 interrompe a conexão representada pela linha pontilhada, e a conexão é reestabelecida pelo enlace de proteção.

A Fig.15a mostra uma rede que não possui enlace de proteção. Quando ocorre uma falha no enlace entre os nós 1 e 2 a restauração dinâmica é executada e um caminho

alternativo é encontrado em torno do enlace da falha, como mostrado na Fig.15b. Os esquemas de proteção e restauração baseados em enlace exibem recuperação mais rápida, mas menos garantida quando desprovidos de fibras de proteção.

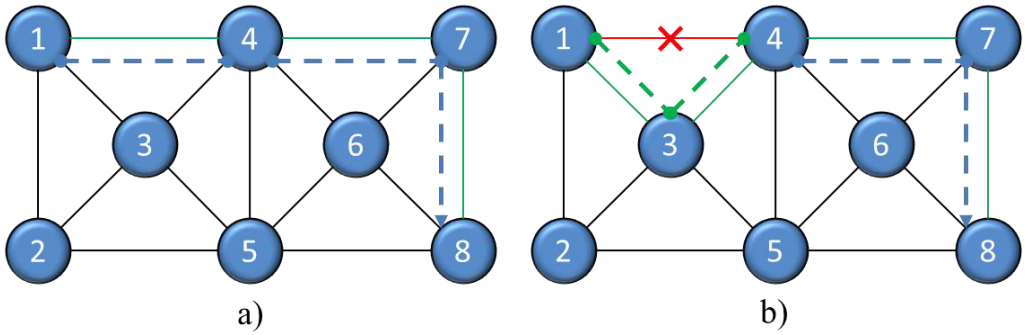


Figura 15 – Restauração baseada no enlace. a) A conexão estabelecida não tem suporte com enlace de proteção; e b) em caso de falha no enlace entre os nós 1 e 2, uma nova rota é estabelecida em torno do enlace da falha.

3.1.2 Atuação em caminho

Em esquemas de proteção e restauração baseadas em caminho, os nós fonte e destino das conexões que transpassam o enlace da falha são sinalizados e um caminho disjunto é utilizado. No caso de um esquema de proteção estática um caminho de proteção é pré-reservado como mostra a Figura 16. Na Fig.16a existem dois caminhos, um que atende à demanda de conexão (pontilhado azul) e outro atua como caminho de proteção (pontilhado cinza). No momento em que ocorre a falha (ver Fig.16b), o caminho de proteção passa a ser utilizado.

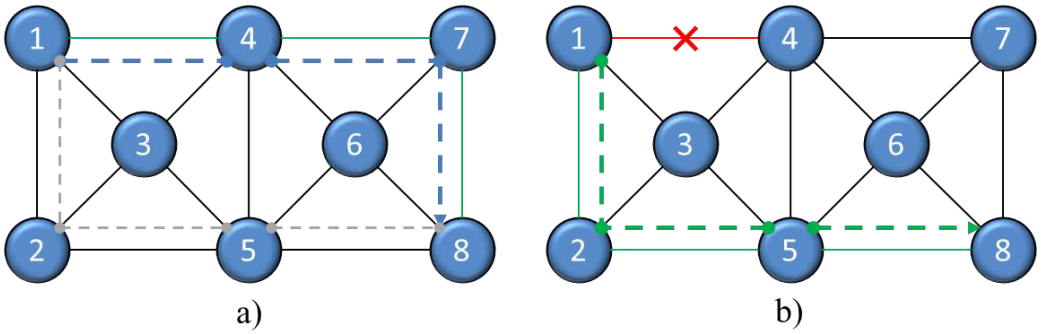


Figura 16 – Proteção baseada em caminho. a) um caminho de proteção (pontilhado cinza) dá suporte a um caminho de trabalho; e b) uma falha no enlace entre os nós 1 e 2 interrompe o caminho de trabalho e o fluxo é encaminhado para o caminho de proteção.

Em um esquema de restauração um novo caminho fim a fim disjunto é computado. A Fig.17a mostra um caminho de trabalho completamente desprovido de proteção. Na ocorrência de falha no enlace entre os nós 1 e 2, o esquema precisa computar uma nova rota a partir das rotas disponíveis na rede, como mostra os traços pontilhados em verde na Fig.17b. A Fig.17c apresenta um exemplo de um caminho de recuperação escolhido que possui o mesmo número de saltos que o caminho de trabalho corrompido. Na Fig.17.d um caminho mais longo é escolhido. No caso de uma restauração, vários caminhos podem ser encontrados e a escolha por um deles depende da heurística utilizada nos algoritmos RSA.

Os esquemas de proteção e de restauração baseados em caminho difere daqueles baseados em enlace porque nos dois casos, o objetivo é recuperar o caminho para garantir a conexão entre o nó fonte e o nó destino, independentemente de qual enlace falhou.

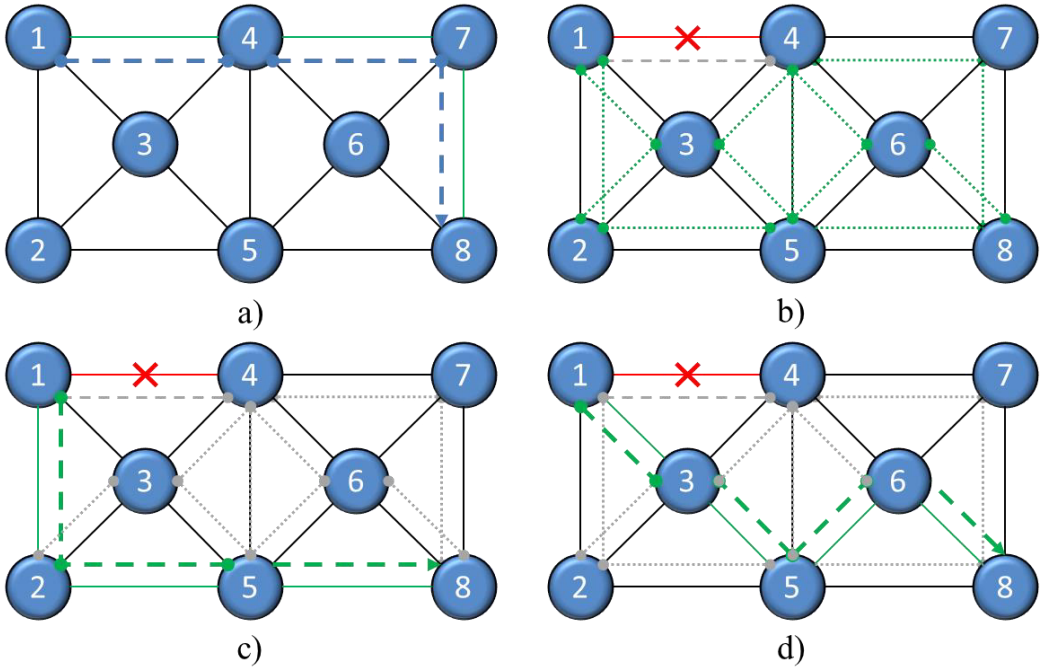


Figura 17 – Restauração baseada em caminho. a) um caminho de trabalho desprotegido; b) ocorre uma falha no enlace entre os nós 1 e 2 que interrompe o caminho de trabalho e uma rota alternativa pode ser traçada utilizando os enlaces disponíveis indicados em verde; c) um caminho de recuperação com mesmo número de saltos é escolhido; d) um caminho de recuperação mais longo é escolhido.

3.1.3 Atuação em subcaminho

Outro escopo de atuação utilizado apenas nos esquemas de restauração é baseado em subcaminho, que é semelhante ao baseado em caminho. A diferença deste tipo de restauração é que parte do caminho é preservada e a outra parte é recalculada. Enquanto na restauração de

caminho ocorre entre os nós fonte e destino, na restauração de subcaminho os nós que participam do processo são o nó anterior ao enlace da falha e o nó destino. A Figura 18 mostra o funcionamento da restauração por subcaminho. Na Fig.18a existe apenas o caminho de trabalho, já na Fig.18b uma falha ocorre no enlace entre os nós 7 e 8. As rotas pontilhadas em verde, presentes na Fig.18b mostram os possíveis subcaminhos que partem do nó anterior à falha (nó 7). Na Fig.18c é escolhido um subcaminho que parte do nó anterior a falha até o nó destino. Já na Fig.18c, outro subcaminho com maior número de saltos é arbitrariamente escolhido. Tanto no caso da Fig.18c quando da Fig.18d, o caminho 1-4-7 é preservado e o subcaminho que parte de 7 até o nó destino é recalculado.

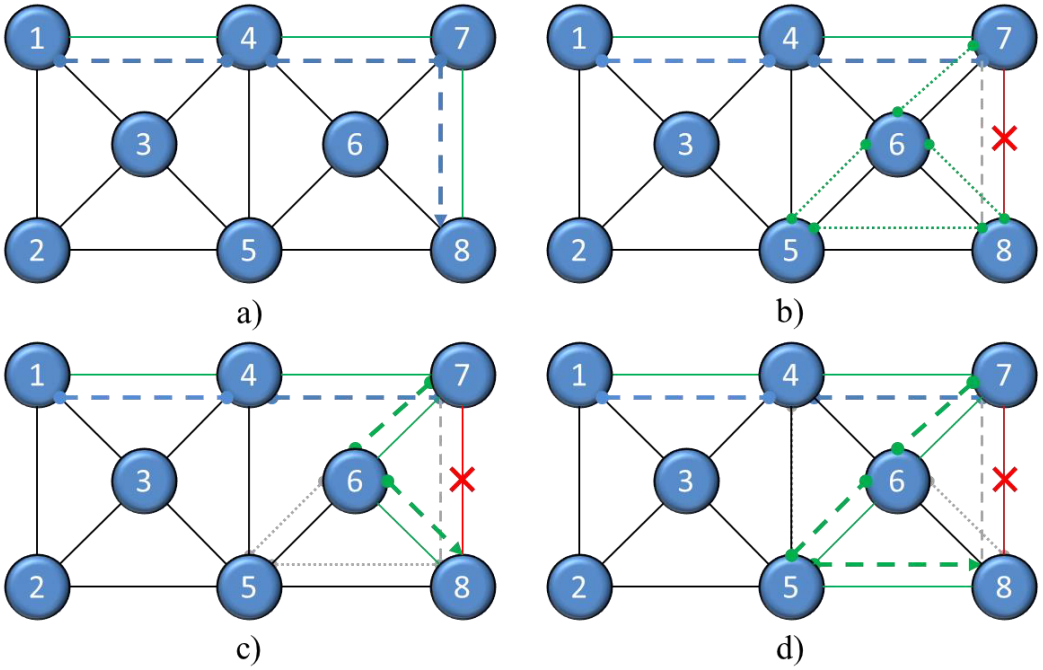


Figura 18 – Restauração baseada em subcaminho. a) um caminho de trabalho desprotegido; b) uma falha no enlace entre os nós 7 e 8 interrompe o caminho de trabalho e os possíveis enlaces que podem constituir a rotas a partir do nó anterior à falha são explicitados; c) um subcaminho é computado entre os nós 7 e 8; d) outro subcaminho com número maior de saltos é computado.

3.2 *Proteção de caminho dedicado* (DPP) 1+1/1:1

O DPP é um esquema de proteção baseado em caminho em que dois caminhos ópticos disjuntos são reservados no momento do estabelecimento da conexão, sendo um o caminho primário e o outro o caminho de proteção. Os caminhos ópticos podem ser disjuntos em enlace ou nó. Um caminho de proteção disjunto em enlace é aquele em que não há enlaces em comum com o caminho primário, mas pode conter nós em comum. Assim, os nós que

transportam o tráfego de múltiplos caminhos primários e/ou de proteção podem ficar congestionados e também a proteção fica vulnerável a falhas oriundas dos nós. Por outro lado, em um caminho de proteção disjunto em nó não existem intersecções entre os conjuntos de nós e nem de enlaces entre o caminho principal e o de proteção, garantindo assim uma melhor distribuição da carga de tráfego e melhor proteção.

Neste esquema de proteção, duas configurações são possíveis: DPP 1+1 e DPP 1:1 [36] e são apresentadas na Figura 19. Na configuração 1+1, uma cópia do sinal de dados é transmitida simultaneamente pelo caminho primário e de proteção como mostra na Fig.19ª. No lado do receptor, o receptor toma a decisão de qual cópia do sinal aceitar com base no QoT. Esta configuração é o esquema de proteção mais rápido disponível, normalmente atuando em algumas dezenas de milissegundos porque não há sinalização envolvida entre os nós do caminho, necessitando apenas que o nó de saída detecte a falha e mude o tráfego para o caminho não afetado. Sendo o regime de proteção mais rápido também é o mais caro em termos de custo, pois utiliza o dobro da capacidade de tráfego, consome mais energia dos *transponders* e demanda uma quantidade maior de fibras instaladas.

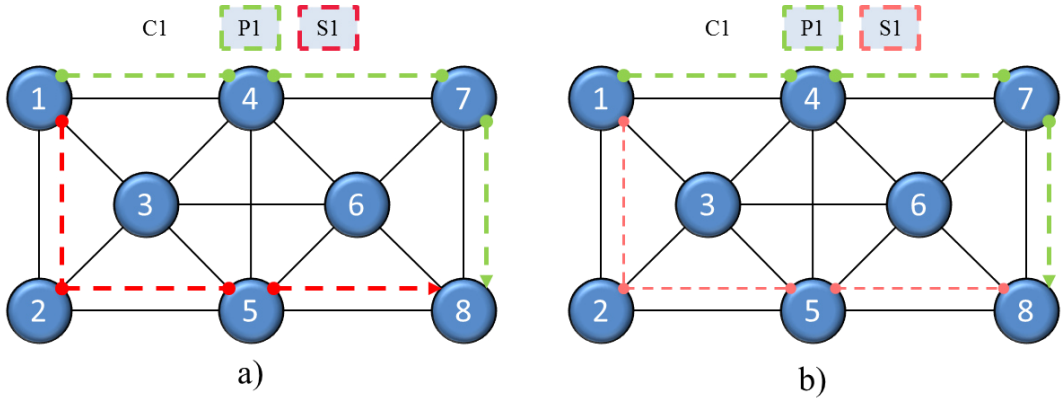


Figura 19 – Exemplos de DPP. a) Configuração DPP 1+1, o sinal é transmitido para a o caminho primário (P1) e secundário (S1) da demanda de conexão (C1). b) Configuração DPP 1:1, o sinal é transmitido apenas para o caminho primário (P1), o caminho secundário mantém-se reservado.

Em contraste com a configuração 1+1, a configuração 1:1 apresentada na Fig.19b transmite os dados apenas no caminho primário enquanto que o caminho de proteção é reservado para utilização futura em caso de falha. No funcionamento normal da rede, o caminho de proteção também pode ser utilizado para a transmissão de tráfego de dados de baixa prioridade. Somente quando ocorre uma falha no caminho primário é que o tráfego no caminho de proteção é interrompido e utilizado para transmitir o tráfego afetado pela falha. Geralmente, esta configuração tem melhor eficiência no uso da capacidade de proteção; no

entanto, ela precisa de uma sinalização entre os nós participantes da falha que muda o tráfego de um caminho para outro, afetando assim a velocidade de restauração. A obtenção de um caminho de trabalho é dado no Apêndice C e o algoritmo DPP é dado no Apêndice D.

3.3 *Proteção de caminho compartilhado* (SPP) 1:N

Assim como o esquema DPP, o esquema SPP também é baseado em caminho. O conceito do SPP é compartilhar um caminho de proteção entre diferentes caminhos primários, ou seja, um caminho de proteção dá suporte a vários caminhos primários. Sob condições normais de funcionamento, considerando que não há falha na rede, o tráfego é transportado apenas pelos caminhos primários; e o caminho de proteção compartilhado só é utilizado quando há falha em caminhos primários [35]. A Figura 20 mostra um exemplo de SPP, na qual os caminhos primários P1 e P2 atendem à demanda de conexão C1 e C2, respectivamente, e dispõem de um caminho disjunto de proteção S1 que dá suporte a ambos.

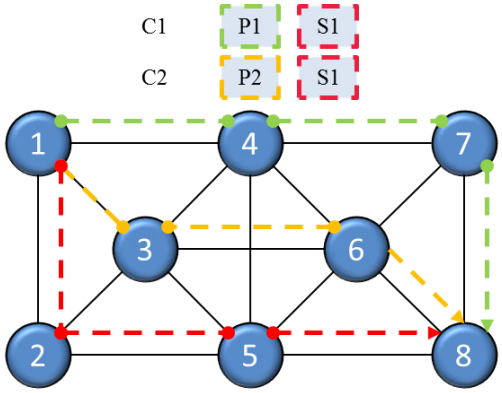


Figura 20 - Exemplo SPP, o caminho secundário (de proteção compartilhada) S1 protege os caminhos primários P1 e P2 das conexões C1 e C2.

O esquema SPP é mais complexo de implementar do que o DPP, porém ele oferece a vantagem de melhorar a utilização dos recursos da rede. Assumindo que todo caminho de trabalho precise de uma proteção, o DPP no melhor dos casos utiliza 50% dos recursos da rede para atender as demandas de conexão e os outros 50% são reservados para caminhos de proteção. O SPP reduz o uso de recursos de proteção compartilhando os caminhos entre caminhos disjuntos [37]. Outra vantagem é que o SPP oferece o mesmo nível de proteção no caso de uma única falha e, para isso, é preciso que algumas restrições sejam respeitadas no momento de estabelecimento do caminho de proteção compartilhado, que são:

1) Que os caminhos de proteção sejam disjuntos de seus respectivos caminhos primários;
2) Que seus caminhos primários também sejam disjuntos entre si;
3) Para caminhos primários que se intersetam em algum enlace, os seus respectivos caminhos de proteção devem ser disjuntos.

Assim, na ocorrência de uma única falha em qualquer nó/enlace da rede, os caminhos primários que transpassam o nó/enlace da falha não concorrem para o estabelecimento da proteção compartilhada, pois eles não compartilham a mesma proteção. A Figura 21 mostra como funciona a reserva de caminhos compartilhados. Na Fig.21a as conexões C1 e C2 utilizam dois caminhos primários P1 e P2 e um de proteção compartilhada S1, disjuntos entre si. Uma nova solicitação de conexão, como na Fig.21b, é alocada para o caminho primário P3. Nesta situação, o caminho de proteção compartilhada S1 não pode dar suporte ao P3, pois seus respectivos caminhos primários P3 e P1 não são disjuntos entre si e, eventualmente, eles poderão concorrer na obtenção da proteção compartilhada. Dessa forma, a solução apresentada na Fig.21c define um caminho de proteção S2 que respeita as restrições dadas.

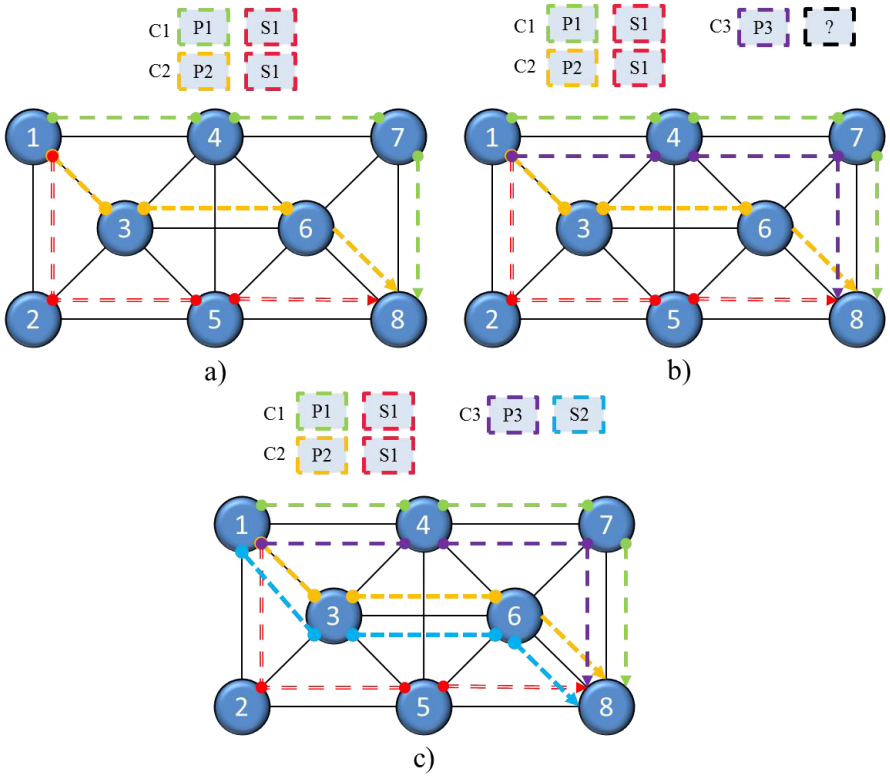


Figura 21 - Exemplo de estabelecimento de um SPP. a) duas demandas de conexão C1 e C2 utilizam dois caminhos primários P1 e P2 e um caminho de proteção compartilhada S1; b) uma nova demanda de conexão C3 é alocada no caminho primário P3; e c) um caminho de proteção S2 é encontrado para P3.

A Figura 22 mostra um exemplo de funcionamento do SPP no caso de ocorrência de uma única falha em enlace. Na Fig.22a, tem-se três demandas de conexão C1, C2 e C3 e seus respectivos caminhos primários P1, P2 e P3 com esquema SPP implementados segundo as restrições dadas. Na Fig.22b, uma falha no enlace entre os nós 4 e 7 afeta os caminhos primários das conexões C1 e C3. Como os caminhos secundários de proteção compartilhada S1 e S2, que dão suporte aos caminhos primários P1 e P3, são disjuntos, a restauração da conexão é feita comutando o fluxo de dados para os seus respectivos caminhos de proteção como mostrado na Fig.22c.

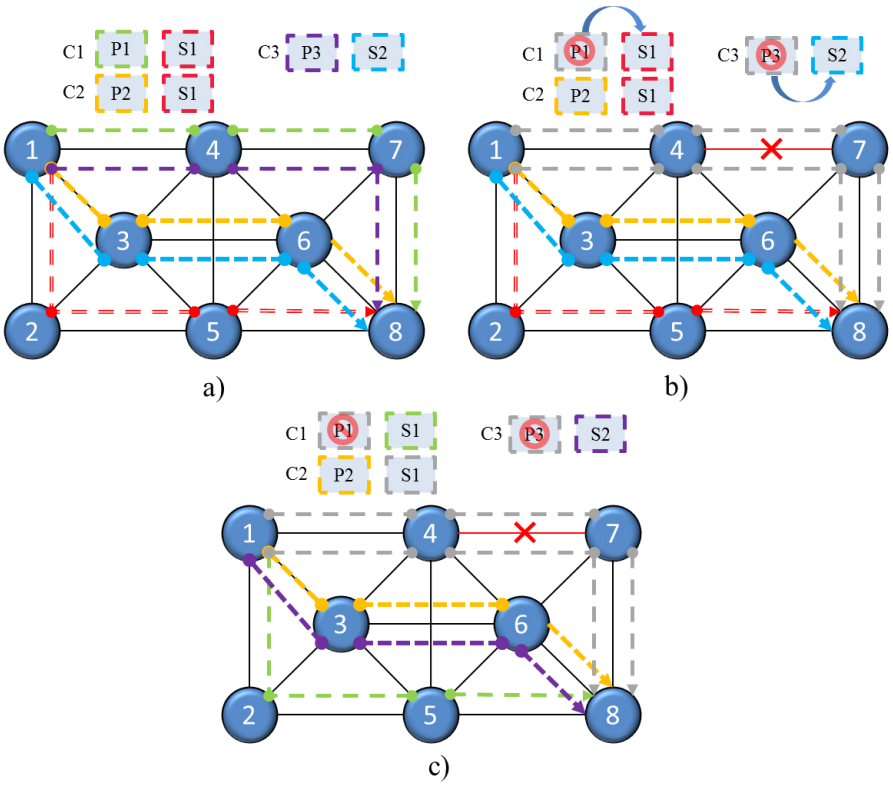


Figura 22 – Exemplo de proteção SPP na ocorrência de uma única falha. a) as demandas de conexão alocadas conforme a Fig.21c; b) uma falha ocorre no enlace entre os nós 4 e 7; e c) os caminhos de proteção S1 e S2 são ativados e restauram as conexões.

3.3.1 SPP *aggressive sharing policy* (ASP)

A grade granular e flexível da EON resulta em um compartilhamento ineficiente para a maioria das implementações do SPP. Em [12], apresenta a abordagem tradicional utilizada em redes WDM chamada de c*onservative sharing policy* (CSP) e a abordagem proposta para EONs chamada de aggressive *sharing policy* (ASP).

O SPP CSP tem a característica de apenas alocar um caminho compartilhado se a largura espectral de seus caminhos é igual, ou seja, precisa haver compatibilidade entre as bandas que se deseja compartilhar. Já o esquema SPP ASP elimina a restrição de compatibilidade de largura de banda e, dessa maneira, os recursos de um caminho de proteção são compartilhados individualmente aumentando a possibilidade de compartilhamento. A Figura 23 apresenta um exemplo de um SPP com as políticas de alocação. A Fig.23a mostra que os recursos de demandas de tamanhos diferentes em um SPP CSP não podem ser compartilhados, resultando um maior consumo de recursos. Na Fig.23b, o SPP ASP permite que demandas de tamanhos diferentes compartilhem individualmente os recursos que

compreendem a intersecção de suas larguras de banda. Assim, o ASP permite aumentar o número de compartilhamentos e reduzir o número de recursos compartilhados na rede.

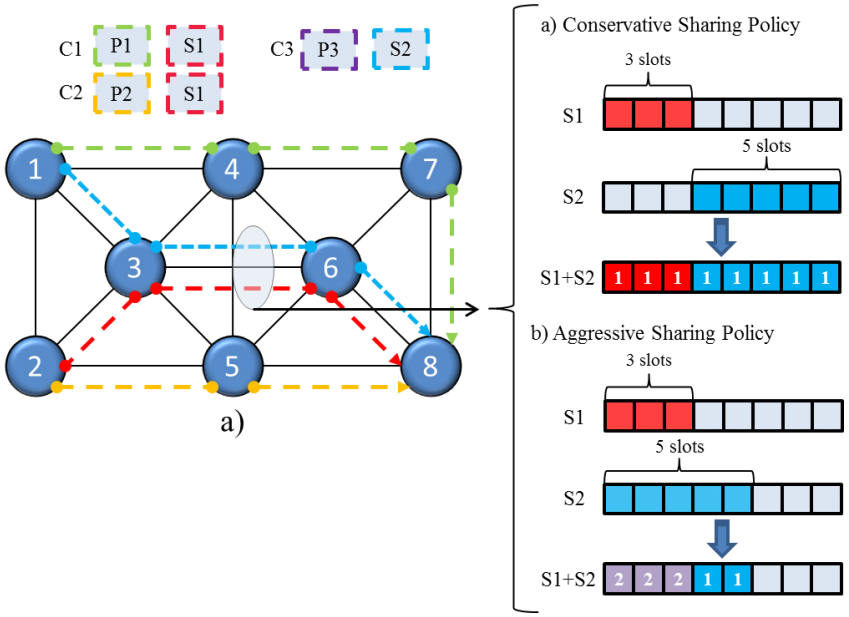


Figura 23 - Exemplo de SPP. a) *conservative sharing policy*; e b) *aggressive sharing policy*.

A obtenção de um caminho de trabalho é dado no Apêndice C e o algoritmo SPP ASP é dado no Apêndice E.

3.4 *Traffic-aware restoration* (TAR)

Em um cenário que ocorrem múltiplas falhas que afeta tanto o caminho primário quanto o caminho de proteção, o tráfego é interrompido, pois ele não pode ser recuperado pelo esquema de proteção e, por isso, inicia-se o processo de restauração dinâmica das conexões afetadas pela falha. Neste processo, um novo caminho de trabalho é computado, chamado de caminho de recuperação, que tenta restabelecer as conexões afetadas pela falha.

Uma característica do tráfego nas EONs é a heterogeneidade das demandas de tráfego, ou seja, com larguras de banda variadas. Um tipo de restauração que utiliza a granularidade das larguras de banda das demandas de conexão como critério é a *traffic-aware restoration* (TAR)[8]. A ideia chave do mecanismo TAR é a classificação do tráfego afetado por prioridade, em que o tráfego de granularidade grossa tem a prioridade mais alta e o tráfego de granularidade fina será recuperado com menor prioridade. Dessa maneira, as novas rotas para

transportar o tráfego afetado podem ser calculadas novamente e as conexões sequencialmente recuperadas de acordo com a sua granularidade.

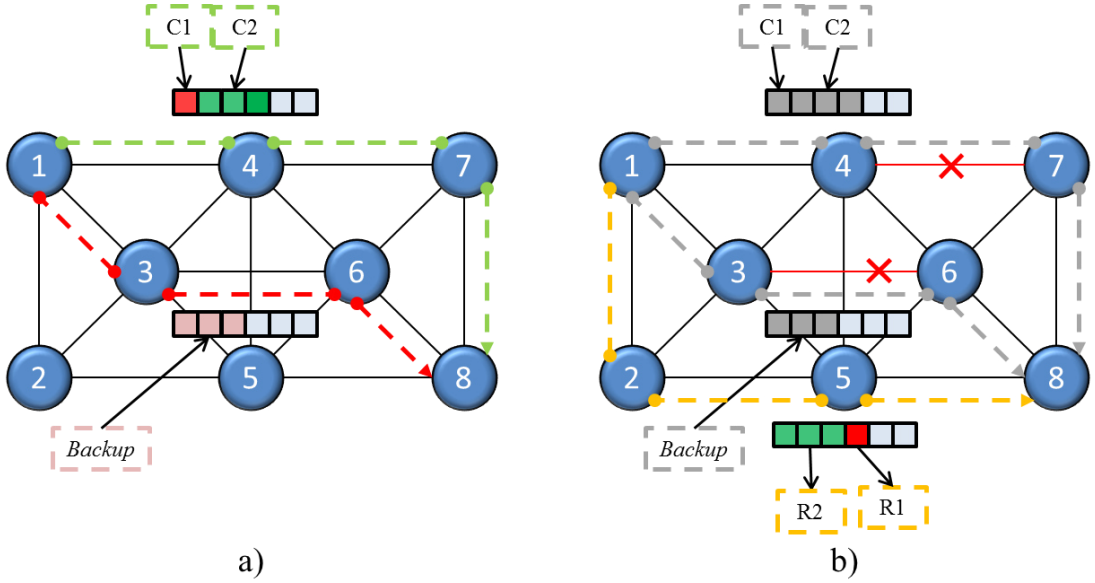


Figura 24 - Exemplo da restauração TAR. a) conexões C1 e C2; e b) as conexões C1 e C2 são recuperadas como R1 e R2 e os espectros alocados de acordo com prioridade de tráfego. Adaptado de [8].

A Figura 24 ilustra um exemplo que considera dois espectros alocados para atender a conexão C1 e C2 pelo caminho formado do nó fonte 1 até o nó destino 8. Na Fig.24a tem-se o caminho primário das conexões alocados na rota 1-4-7-8 e o caminho de proteção alocado na rota 1-3-6-8. Se uma falha ocorrer simultaneamente no enlace do caminho primário e do caminho de proteção, como mostra a Fig.24b, se dependesse apenas do mecanismo de proteção as conexões não poderiam ser restauradas e seriam desconectadas. Porém, se for aplicado o mecanismo TAR, pode-se reencaminhar C1 e C2 pela rota 1-2-5-8 e alocá-las conforme a classificação de prioridade. Assim, as conexões C1 e C2 que foram afetadas pelas falhas são recuperadas e correspondem respectivamente a R1 e R2. Como o espectro de C2 é maior do que o do espectro de C1, então a sua conexão recuperada R2 tem maior prioridade e é alocado primeiro, e depois é alocada a conexão recuperada R1.

3.5 *Bandwidth squeezing restoration* (BSR)

As redes elásticas podem utilizar o recurso *bandwidth squeezing restoration* (BSR). O conceito BSR proposto em [9] é baseado em supervisão de tráfego (*traffic policing*) de rede. *Traffic policing* é o processo de monitoramento de tráfego de rede para o cumprimento de um

acordo de serviço entre o provedor e de serviços e o cliente. Esse acordo é chamado de *service-level agreement* (SLA), e nele alguns critérios podem ser incluídos como serviços a serem entregues, desempenho do serviço prestado, gerenciamento de falhas e segurança [38].

Entre os itens citados está o critério de desempenho. Uma das medidas de desempenho em um SLA é a taxa de bits do serviço, que permite definir perfis de tráfego diferenciados na rede. O perfil de tráfego é dado pelo algoritmo *two-rate three-color marker* [39], originalmente proposto para redes orientadas a pacotes, o qual define dois limiares chamados de "*commited rate*" e "*excess rate*". Esses limiares são usados para marcar os pacotes com cores e diferenciá-los em três níveis de prioridade de tráfego. Os pacotes enviados em taxas que excedem o limiar "*excess rate*" são marcadas com a cor vermelha e possuem alta probabilidade de serem descartados. Os pacotes que são enviados em taxas entre a "*commited rate*" e "*excess rate*" são marcados com a cor amarela e têm menor probabilidade de descarte do que os marcados com vermelho. Por fim os pacotes que são enviados em taxas abaixo do "*commited rate*" são marcados de verde e têm a menor probabilidade de descarte das três. Com base no algoritmo, duas políticas de tráfego podem ser utilizadas para redes ópticas:

1. A primeira permite que a largura de banda exceda o limiar de "*excess rate*" no caso de disponibilidade de banda. Este é o caso que pode ser aplicado nas redes WDM de grade fixa quando a taxa de bits contratada é menor que a taxa de bits de um comprimento de onda inteiro alocado;
2. A segunda política permite apenas que a largura de banda exceda a "*commited rate*". Neste tipo de política a largura de banda extra é alocada pela política do melhor esforço (*best-effort policy*), ou seja, apenas será alocado se houver disponibilidade de banda, caso contrário será alocado apenas a largura de banda comprometida.

Nas redes com comutação de circuitos, especialmente nas EONs, não há necessidade de um algoritmo que controla a taxa de bits, uma vez que não há envio de pacotes e sim uma banda que é alocada a um espectro flexível de tamanho arbitrário que naturalmente acomoda a demanda de tráfego desejada. Utilizam-se então apenas os conceitos dos limiares de banda dos níveis de serviços a fim de explorar a característica da elasticidade de banda das EONS em esquemas de proteção e restauração. Dessa forma, quando ocorre uma falha no caminho primário, a conexão é encaminhada para o caminho de proteção que pode ter a sua largura de banda reduzida para taxa mínima requerida. Isto garante melhor utilização dos recursos e grande capacidade de sobrevivência da rede até mesmo em um cenário de múltiplas falhas.

Esse tipo de restauração que tem como característica principal a contração da banda de proteção dá-se o nome de *bandwidth squeezing restoration* (BSR).

Neste esquema existem três possíveis modelos de comportamento de recuperação de dados: *full bandwidth guaranteed recovery* (FBGR), *partial bandwidth guaranteed recovery* (PBGR), *best effort recovery* (BER). Esses modelos são determinados com base na função de alocação de largura de banda especificada (*specified bandwidth allocation function*) e na função de alocação de banda por melhor esforço (*best-effort bandwidth allocation function)* [10]. A Figura 25 ilustra a capacidade de largura de banda alocada em cada modelo e utilização das funções de alocação.

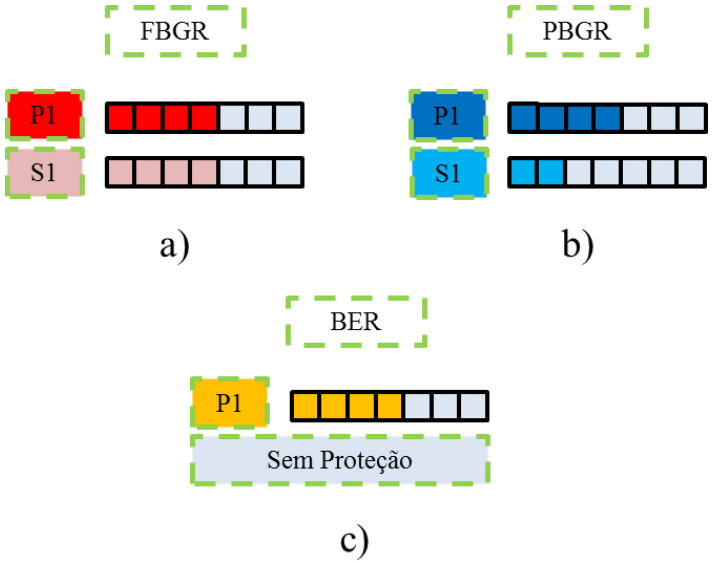


Figura 25 – Níveis de serviço na alocação. a) FBGR com restauração completa. b) PBGR com 50% de contração de banda. c) BER, não há proteção reservada. Adaptado de [10].

A função de alocação de largura de banda especificada predefine a quantidade de banda que será pré-reservada e tem como base o esquema DPP. Essa quantidade é definida independentemente dos recursos disponíveis na rota de recuperação. Dessa maneira, os padrões FBGR e PBGR decidem a largura de banda do caminho de recuperação antes de alocar o caminho primário. O FBGR aloca um caminho de recuperação com a mesma quantidade de banda do caminho primário (Fig.25a), ou seja, nele não há contração de banda, e isso corresponde a um esquema de proteção DPP tradicional. Já o PBGR aloca um caminho de recuperação com a quantidade de banda especificada pela banda garantida, que é uma parcela da banda ocupada pelo caminho primário. No exemplo de PBGR apresentado na Fig.25b, a função de alocação de banda funciona como um DPP que aloca 50% da largura de

banda especificada. Na função de melhor esforço não há tal reserva. Os caminhos primários alocados com o padrão BER são dinamicamente restaurados após a ocorrência da falha (Fig.25c). Neste cenário, a quantidade de banda necessária é alocada de acordo com a disponibilidade de recursos que pode ser reduzida até a granularidade mínima da rede. Nesse trabalho, o esquema BSR não é comparado com outros esquemas devido a sua dependência com os níveis de serviços escolhidos para as conexões do cliente, por isso, a comparação é realizada com os diferentes proporções de níveis de serviços que implementam os respectivos modelos estudados.

4 ALGORITMOS RSA

O problema RSA tem complexidade NP-*hard*, como provado em [6] e, por isso, podem existir mais de uma solução que, se forem resolvidas pela busca exaustiva (solução exata), o custo computacional seria alto, mesmo para pequenas redes. Por esse motivo, resolver um problema RSA não se resume apenas em encontrar uma solução, mas sim uma solução ótima ou próxima da ótima com base em determinados critérios e, portanto, ele é um problema de otimização. Com esse objetivo são utilizadas heurísticas, que são um conjunto de regras e métodos que conduzem à descoberta de uma solução que tende a maximizar ou minimizar uma determinada função objetivo. Além do mais, a solução conjunta do problema RSA possui um espaço de busca muito grande e pode ser reduzida separando-o em dois subproblemas: roteamento e alocação de espectro. Neste estudo, é utilizado o algoritmo de *Dijkstra* para resolver o subproblema de roteamento e o algoritmo *first-fit* para o subproblema de alocação de espectro. Ambos os algoritmos são heurísticos, sendo que o primeiro encontra o menor caminho (*shortest path*) em um grafo e o segundo encontra o primeiro encaixe no qual caiba o espectro requerido. Tendo em vista essa solução base (*Dijkstra+first-fit*), podem-se ainda utilizar heurísticas adicionais que alterem a função objetivo da solução. Neste sentido, são propostas duas heurísticas que consideram os caminhos de proteção compartilhados (SPP *aware*). A primeira heurística, proposta em [8], é o *dynamic load balancing shared-path protection* (DLBSPP), que resolve o subproblema de roteamento com balanceamento de carga nos enlaces na computação dos caminhos primários e caminhos de proteção compartilhados. A segunda heurística, nomeada *inverted dual stack* (IDS) resolve o subproblema de alocação de espectro com o objetivo de maximizar o número de compartilhamentos dos recursos de proteção compartilhada.

Nesta seção apresenta-se o algoritmo de *Dijkstra* para tratar o subproblema de roteamento e a heurística DLBSPP, bem como a técnica utilizada para obtenção dos caminhos disjuntos e em seguida o algoritmo *first-fit* para tratar o subproblema de alocação de espectro e a heurística de alocação IDS.

4.1 O subproblema de roteamento

Uma topologia de rede é representada por um grafo $G(V, L)$, em que o conjunto $V = \{v_1, v_2, v_3, \dots, v_n\}$ denota os vértices que representam os nós da rede e $L = \{l_1, l_2, l_3, \dots, l_m\}$ é o conjunto de arestas que representam os enlaces da rede, sendo que os

valores n e m correspondem respectivamente ao número máximo de nós e enlaces. A proporção entre quantidade de arestas e vértices representa densidade de um grafo. Para determinada quantidade de vértices, um grafo é dito denso quando possui muitas arestas e esparso quando possui poucas. Uma rota é definida por um conjunto $R = \{r_1, r_2, \dots, r_c\}$, tal que $R \subseteq V$. O processo de roteamento consiste em encontrar o conjunto R de elementos não repetidos que satisfaça a conectividade dos vértices, ou seja, que para cada par de elementos (r_i, r_{i+1}) da rota exista um enlace correspondente em L. Para a solução do subproblema de roteamento apresenta-se o algoritmo de *Dijkstra* e em seguida a heurística DLBSPP que otimiza a computação de caminhos primários e de proteção compartilhada. Por fim é apresentado o procedimento de computação dos caminhos disjuntos que é uma condição necessária para obtenção dos caminhos de proteção.

4.1.1 O algoritmo de Dijkstra

O algoritmo utilizado nesse trabalho é o de Dijkstra, publicado em 1959 pelo cientista da computação holandês Edsger W. Dijkstra, cujo artigo "*A note on two problems in connexion with graphs*" [40] apresentava dois algoritmos para a solução de dois problemas teóricos com grafos: o problema de árvore de extensão mínima (*minimum weight spanning tree*) e o problema do caminho mais curto (*shortest-path*). Hoje, o algoritmo de Dijkstra para o problema do caminho mais curto é um dos algoritmos mais conhecidos em ciência da computação e um algoritmo muito popular em pesquisa operacional.

O algoritmo de Dijkstra soluciona o problema do caminho mais curto em um grafo dirigido ou não dirigido com arestas de peso não negativo. O algoritmo utiliza a estratégia de busca em largura (*breadth-first search*, BFS) e o seu caráter heurístico é considerado como de um algoritmo guloso (*greedy algorithm*), ou seja, um algoritmo heurístico que a cada passo seleciona a melhor opção disponível naquele passo sem levar em conta resultados futuros.

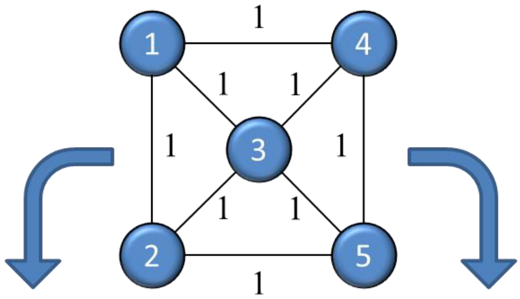
A solução do algoritmo é construída definindo um conjunto S de menores caminhos formado a partir do vértice inicial I. A cada passo do algoritmo busca-se nas adjacências dos vértices pertencentes a S aquele vértice com menor distância relativa a I. A seguir, aquele vértice é adicionado à S e repetem-se os passos até que todos os vértices alcançáveis por I estejam incluídos em S.

A complexidade do algoritmo Dijkstra depende do tipo de implementação utilizada. Considere um grafo de V vértices e L arestas, assim a complexidade de cada implementação do algoritmo é dado a seguir [41]:

1) Dijsktra ingênuo. Esta é a implementação mais simples, porém ineficiente. Na implementação ingênua o tempo computacional é proporcional a VL, mas como L no pior caso é proporcional a V^2 então a complexidade do Dijkstra ingênuo é $O(V^3)$;
2) Dijkstra para grafos densos: Esta implementação consome tempo proporcional $V^2 + L$. Como $L < V^2$, então a complexidade é $O(V^2)$.
3) Dijkstra para grafos esparsos: Esta implementação utiliza fila priorizada para ordenar o vetor de distância relativa. Se a fila de prioridade for implementada como um *heap*, todas as operações sobre a fila podem ser executadas em tempo limitado por $\log(V)$. Nesse caso, a implementação consome tempo proporcional a $(\mathrm{V} + \mathrm{L})\log(V)$ no pior caso. Se o grafo for fracamente conexo então $L \geq \mathrm{V} - 1$ e portanto o consumo de tempo é proporcional a $\mathrm{O}(\mathrm{Alog}(V))$

Caso a topologia de rede seja restringida a grafos esparsos, a implementação Dijkstra para grafos esparsos é assintoticamente mais rápida do que para grafos densos. Mas, se o grafo é denso então a implementação para grafos densos é mais rápida.

Outra variação na implementação do algoritmo é o tipo de representação do grafo utilizada. Os grafos podem ser representados por matriz de adjacência ou por lista de adjacência como mostra a Figura 26. Na Fig.26a, o grafo não direcionado é representado por uma matriz de adjacência e cada elemento representa o custo de cada aresta. Já na Fig26b o grafo é representado por lista de adjacência, sendo que cada nó apresenta uma lista de outros nós com que estão conectados. A representação por matriz de adjacência apresenta duas vantagens: não requer nenhuma estrutura de dados adicional e o acesso ao custo do enlace é direto. Na representação por lista de adjacência, que normalmente é implementada por uma estrutura de *linked-list*, o acesso ao elemento resulta em uma busca sequencial e o elemento deve conter uma estrutura de dados que guarde o custo do enlace.



$$\begin{bmatrix} Inf & 1 & 1 & 1 & Inf \\ 1 & Inf & 1 & Inf & 1 \\ 1 & 1 & Inf & 1 & 1 \\ 1 & Inf & 1 & Inf & 1 \\ Inf & 1 & 1 & 1 & Inf \end{bmatrix}_{V \times V}$$

a)

$$\begin{cases} 1 \rightarrow & \{2 \quad 3 \quad 4\} \\ 2 \rightarrow & \{1 \quad 3 \quad 5\} \\ 3 \rightarrow & \{1 \quad 2 \quad 4 \quad 5\} \\ 4 \rightarrow & \{3 \quad 4 \quad 5\} \\ 5 \rightarrow & \{2 \quad 3 \quad 4\} \end{cases}$$

b)

Figura 26 - Representação dos grafos: a) por matriz de adjacência e b) por lista de adjacência.

A implementação do algoritmo de Dijkstra utilizada nesse trabalho é para grafos densos e com representação por matriz de adjacência. O pseudocódigo do algoritmo é descrito no Apêndice A.

4.1.2 Dynamic load balancing shared-path protection (DLBSPP)

O DLBSPP apresentado em [8], é uma heurística de roteamento que considera o balanceamento dinâmico de carga na computação do caminho, ou seja, os enlaces menos carregados são preferidos na computação tanto do caminho primário (1) quanto no caminho de proteção (2) para uma demanda de conexão. Os espectros livres são reservados apenas para os caminhos primários. Contudo, com base no princípio do compartilhamento de recursos espectrais para o caminho de proteção, a reserva desses recursos depende dos recursos reservados para proteção e dos recursos livres. Portanto, considerando a diferença de recursos do espectro reservado entre caminho primário e caminho de proteção, duas diferentes funções de custo é adotada para atualizar a matriz de custo do enlace (matriz de adjacência), pelo qual o caminho primário e de recuperação escolhidos possam ser otimizados. A função de custo para computação do caminho primário (1) deve escolher o caminho mais curto, desde que todos os enlaces ao longo do caminho tenham mais recursos livres. Durante o processo de calcular o caminho primário de menor custo, são preferidos os enlaces pouco carregados.

Assim, o estado de desequilíbrio de carga de rede, em que os recursos espectrais disponíveis em alguns enlaces são excessivamente consumidos, pode ser evitado. A Tabela 4 apresenta algumas definições necessárias para computar (1) e (2) [8].

Tabela 4: Variáveis utilizadas pelo algoritmo DLBSPP [8]

Variável	Descrição
$L_{i,j}$	O enlace entre o nó i e j
$W_{i,j}$	O custo base de cada enlace $L_{i,j}$
$BS_{i,j}$	O número de *slot* de frequência do caminho de recuperação consumido no enlace $L_{i,j}$
$FS_{i,j}$	O número de *slot* de frequência livres no enlace $L_{i,j}$
$DW_{i,j}$	O custo dinâmico do caminho primário no enlace $L_{i,j}$
$BW_{i,j}$	O custo dinâmico do caminho de recuperação no enlace $L_{i,j}$
α	> 1
β	> 1

$$DW_{i,j} = \begin{cases} \infty, \ Se\ FS_{i,j} = 0 \\ \frac{\alpha}{FS_{i,j}} W_{i,j}, \ Se\ FS_{i,j} > 0 \end{cases} \quad (1)$$

$$BW_{i,j} = \begin{cases} \infty, & Se\ FS_{i,j} = 0\ e\ BS_{i,j} = 0 \\ \frac{\alpha}{FS_{i,j} + \beta BS_{i,j}} W_{i,j}, & caso\ contrário \end{cases} \quad (2)$$

Um exemplo de como as funções de custo permitem o balanceamento na computação do caminho é dado na Figura 27. Na Fig.27a a computação do caminho primário é feita pelo menor caminho entre o nó fonte 1 e o nó destino 7. Os custos dos enlaces são todos iguais a 1 e a cada alocação de caminho permanece inalterado. Na Fig.27b os custos dos enlaces são calculados por (1) a cada alocação de caminho. No primeiro momento não há caminho alocado, portanto o custo de todos os enlaces é 1. Após o primeiro menor caminho ser computado e alocado, os custos são atualizados. Na segunda computação, o menor caminho encontrado seleciona enlaces com menor custo, ou seja, enlaces menos carregados.

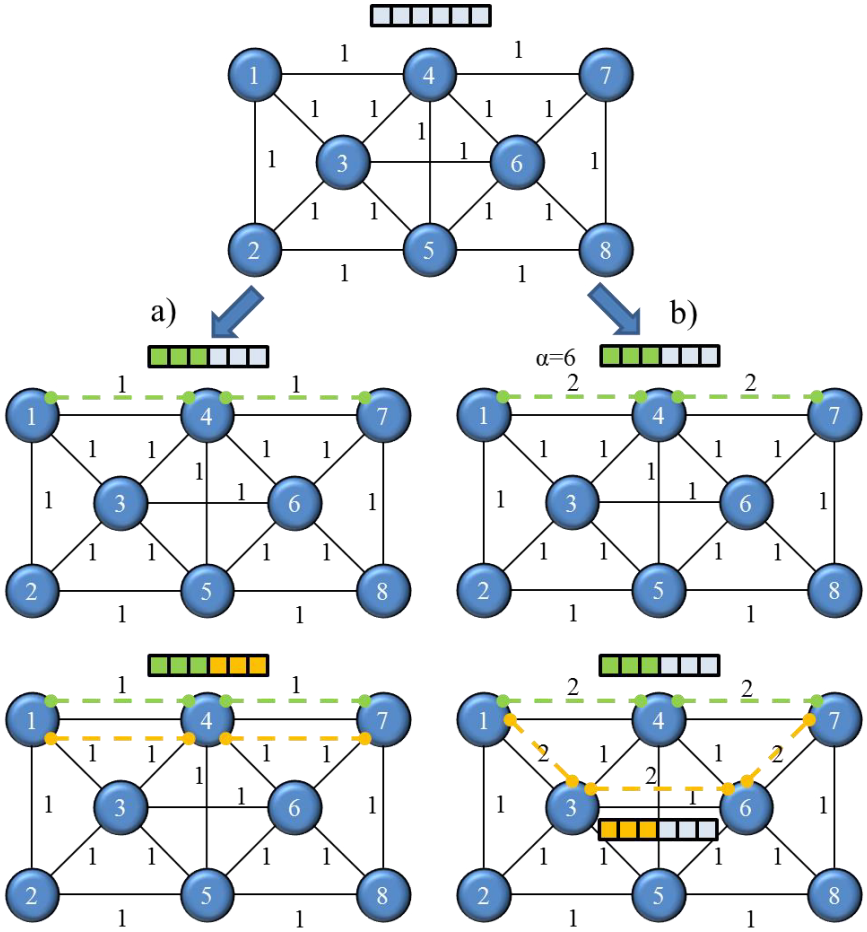


Figura 27 - Exemplo de balanceamento de carga para alocação do caminho primário do nó fonte 1 ao nó destino 7. Dada uma topologia de rede inicial têm-se: a) alocação do menor caminho utilizando custo básico em cada enlace; b) alocação do menor caminho com os custos balanceados por (1).

4.1.3 Obtenção dos caminhos disjuntos

No processo de roteamento, a obtenção de um caminho que seja disjunto a outro caminho é importante para definir os caminhos de proteção. Existem dois tipos de caminhos disjuntos: em nó e em enlace. Suponha uma topologia em malha com 5 nós e um caminho principal “1-3-5” como mostrado na Figura 28. Um caminho disjunto em nó (Fig.28a) são todos aqueles caminhos possíveis em que a interseção de seus nós intermediários com os nós intermediários do caminho principal é o conjunto vazio, ou seja, os nós intermediários do caminho principal não estão contidos nos nós intermediários do seu caminho disjunto em nó. Nesse exemplo, observa-se que o nó fonte e destino podem estar contidos em ambos os caminhos. Por outro lado, um caminho disjunto em enlace pode conter os nós intermediários do caminho principal, porém não contém os pares de nós que representa o enlace do caminho

principal. Na Fig.28b todos os possíveis caminhos não contêm o enlace “1-3” e nem o “3-5”, embora alguns caminhos possam conter o nó intermediário “3”.

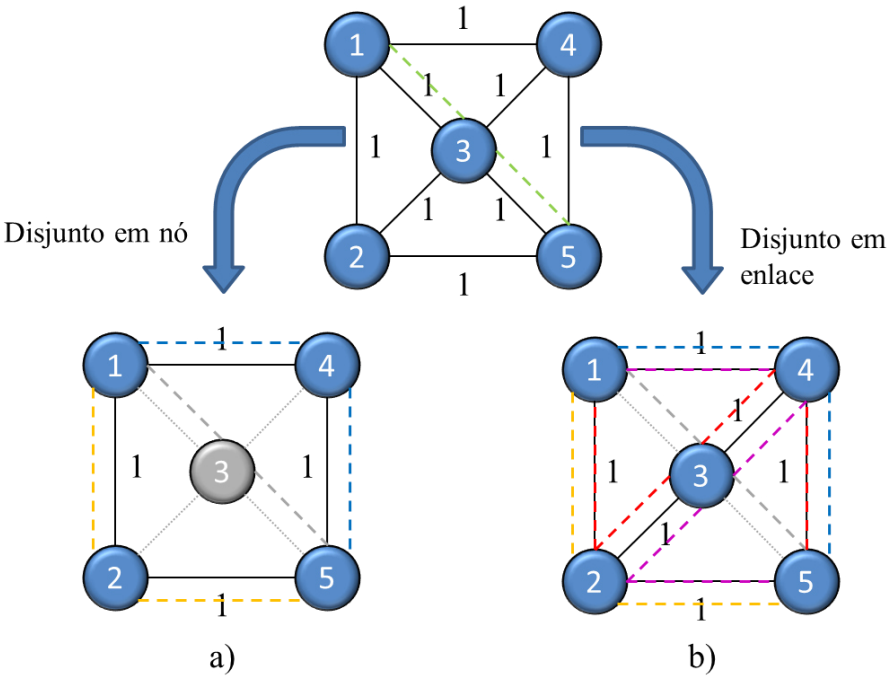


Figura 28 - Caminhos disjuntos em: a) nó, b) enlace.

Os caminhos disjuntos são obtidos alterando a matriz de adjacência que representa a topologia de rede e, dessa forma, o algoritmo de roteamento é capaz de encontrar naturalmente um caminho disjunto, seja em nó ou em enlace, do caminho principal. Na Figura 29 apresentam-se as operações necessárias para a obtenção de cada tipo de caminho disjunto. A Fig.29a mostra a matriz de adjacência para obtenção de um caminho disjunto em nó. Nesse processo, as linhas e colunas da matriz referente aos nós intermediários são anuladas, ou seja, para cada elemento pertencente às linhas e colunas anuladas, é atribuído o valor infinito. No caso da obtenção de um caminho disjunto em enlace na Fig.29b, os elementos que correspondem aos enlaces contidos no caminho principal são anulados. Nesse exemplo, assume-se que os enlaces são bidirecionais, dessa forma o rompimento de um enlace compromete o tráfego em ambas as direções e, por isso, são anulados também os elementos diagonalmente espelhados na matriz, ou seja, para os elementos “1-3” e “3-5”, são também anulados os elementos “3-1” e “5-3”.

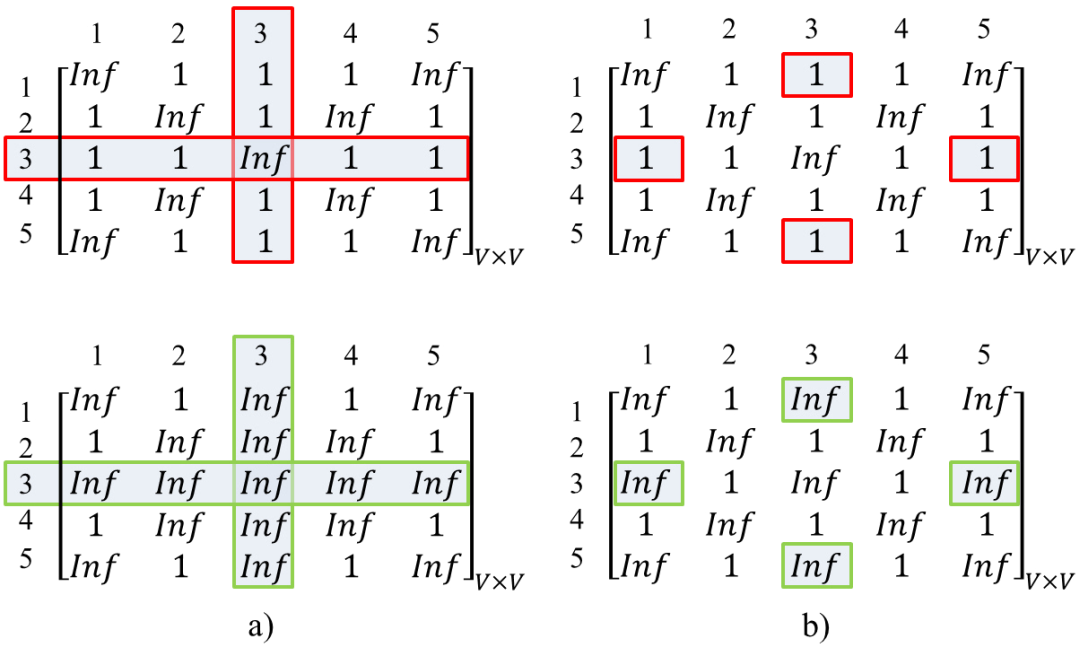


Figura 29 - Modificação da matriz de adjacência para obtenção de caminhos disjuntos em: a) nó e b) enlace.

4.2 O subproblema de alocação de espectro

Os algoritmos de alocação têm origem nos estudos de sistemas operacionais de computadores, especificamente quanto ao gerenciamento de memória. Como mostrado na Seção 2.1, o espectro é discretizado em pequenas porções capazes de alocar uma banda. Na abstração lógica do plano de controle, cada subportadora pode ser análoga a uma posição de memória como nos sistemas operacionais. Dessa forma, o conjunto de subportadoras do espectro utilizável é representado por um conjunto de blocos lógicos $F = \{f_1, f_2, f_3, \dots, f_k\}$, em que cada elemento é chamado de *frequency slot unit* (FSU) e o valor de k representa o número máximo de FSUs que compõe o espectro. A Figura 30 mostra a abstração do espectro em blocos lógicos.

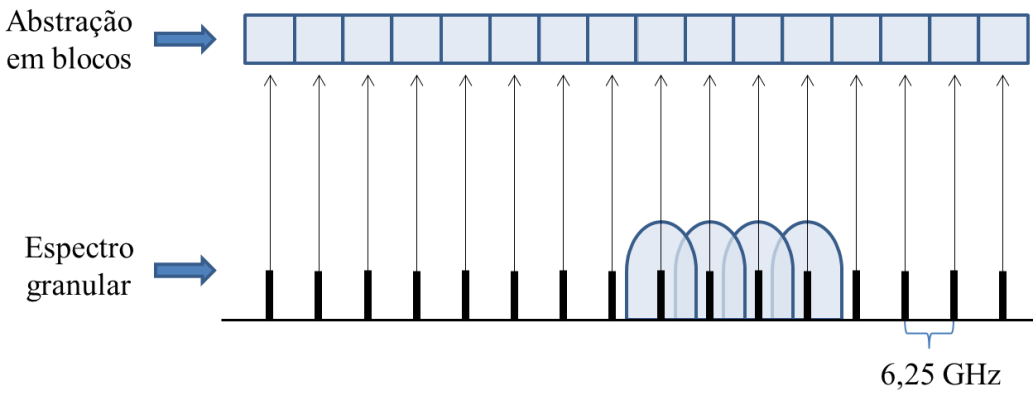


Figura 30 - Abstração em blocos do espectro granular.

4.2.1 Algoritmo *first fit* (FF)

O algoritmo de alocação FF é um dos algoritmos utilizados em sistemas operacionais para decidir em que local da memória deve ser alocado um processo. Ele funciona escolhendo sempre o primeiro espaço vazio na memória no qual caiba o processo. Neste algoritmo existe um gerenciador de blocos de memória chamado de alocador. O alocador mantém uma lista de blocos livres (conhecida como "*free-list"*) e, ao receber um pedido de memória, examina a lista e avalia se o bloco livre é suficiente para alocar o bloco requerido. Se o bloco escolhido for igual ao requerido, então o processo é alocado neste bloco e a sua referência removida da "*free-list*". Caso o bloco escolhido seja maior do que o requerido, o alocador recalcula a diferença que restou no bloco livre da "*free-list*". Enquanto o bloco escolhido for menor que o bloco requerido, a busca continua até encontrar um espaço de encaixe ou alcançar o fim da memória. Dessa forma, o algoritmo FF pode ser implementado de duas maneiras, a primeira implementação utiliza uma estrutura de *linked-list* para guardar os blocos. A operação de busca em uma *linked-list* tem complexidade $O(N)$. A segunda implementação utiliza uma estrutura de árvore binária balanceada, em que os blocos são ordenados segundo seu tamanho e valor base e tem complexidade $O(\log(N))$.

O funcionamento do FF é apresentado na Fig.31. Na Fig.31a, Fig.31b e Fig.31c são realizadas alocações sequenciais de banda no sentido indicado pelas flechas. Na Fig.31d o espectro vermelho é liberado deixando dois blocos livres. Na alocação seguinte na Fig.31e, a demanda de quatro blocos não cabe no primeiro conjuntos de blocos livres deixado pela alocação anterior, então essa demanda é alocada no próximo conjunto de blocos livres. Na Fig.31e a demanda de três blocos não cabe no único conjunto de blocos livres restante então essa demanda é bloqueada.

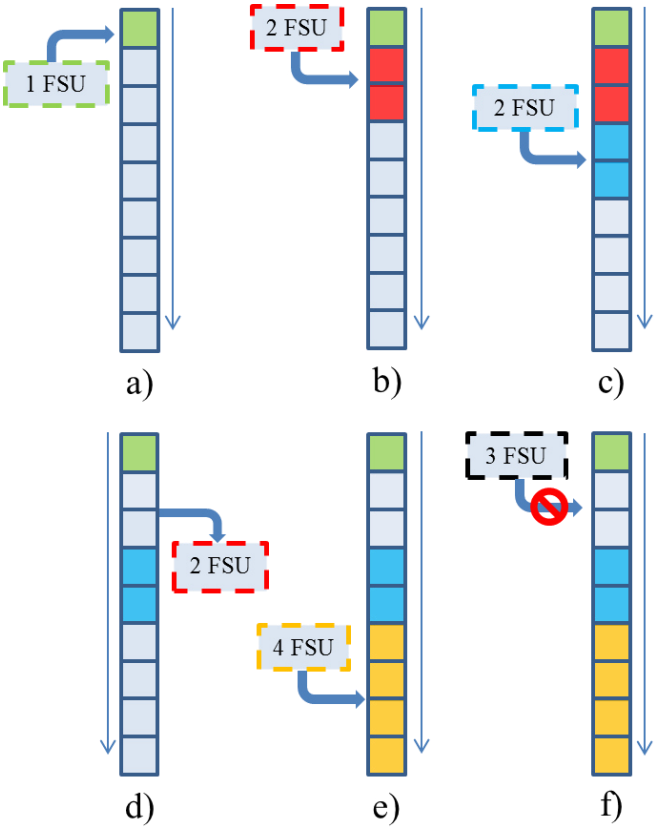


Figura 31 - Exemplo de alocação FF. a) alocação de 1 FSU, b) alocação de 2 FSUs, c) alocação de mais 2 FSUs , d) a alocação vermelha de 2 FSUs é liberada. e) uma demanda de 4 FSUs é alocado no primeiro conjunto livre que acomoda a demanda. f) a demanda de 3 FSUs não cabe no espectro é bloqueada.

O processo de alocação se torna mais complexo quando a busca precisa ser realizada considerando múltiplos enlaces. Dado um caminho de rede, a sequência de enlaces que compõe o caminho é alinhada de forma que, respeitando as restrições de continuidade e consecutividade dos blocos, seja efetuada uma busca sequencial em duas dimensões, como mostrado na Figura 32. Supondo uma rede com V nós, o número máximo de saltos é proporcional a V, portanto a complexidade do algoritmo de alocação para duas dimensões passa a ser $O(VN)$ e $O(Vlog(N))$, respectivamente, para a implementação com *linked-list* e árvore binária.

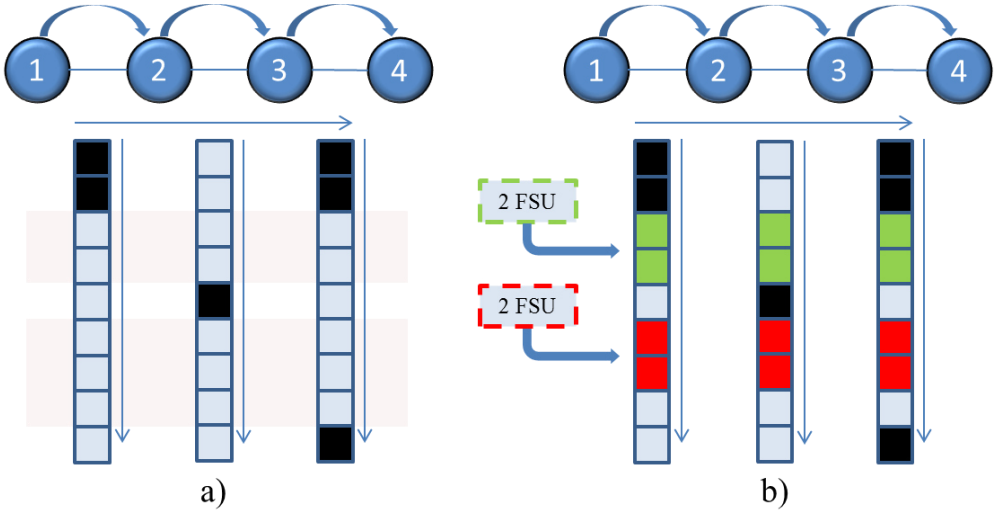


Figura 32 - Alocação de espectro considerando múltiplos enlaces. a) Estado inicial de alocação dos enlaces. b) Alocação de duas demandas de conexão.

Nesse trabalho é utilizada a implementação do algoritmo FF sequencial, que possui mesma complexidade da implementação em *linked-list*, a diferença é que cada FSU é obtido e avaliado por vez. Essa tipo de implementação foi escolhido devido à facilidade de controlar individualmente os atributos de cada FSU por meio dos indexadores na varredura bidimensional, dessa forma, facilita também a implementação da versão *first-fit* inverso utilizada na heurística apresentada na Seção 4.2.2. O pseudocódigo do algoritmo de alocação FF é descrito no Apêndice B.

4.2.2 Inverted dual stack (IDS)

A heurística *inverted dual stack* (IDS) é inspirado no esquema de organização de memória de computadores. O gerenciamento de memória em computadores consiste em organizar e alocar os blocos de memórias necessários para execução do sistema operacional e dos processos. Assim, os algoritmos de alocação como o FF são estudados nos esquemas de gerenciamentos de memória em sistemas operacionais. Uma das maneiras mais simples utilizada para organização da memória é dividindo-a em dois segmentos, um reservado para alocar o sistema operacional e outro para o processo. Esta é maneira utilizada em sistemas monoprogramados, ou seja, sistemas que permitem que apenas um processo seja executado por vez, por exemplo, em alguns sistemas embarcados. No caso de sistemas multiprogramados, o segundo segmento é utilizado para alocar múltiplos processos, e a quantidade de memória alocada em cada um depende do tamanho do programa em disco. Um programa é um conjunto de dados gravado em disco, quando um programa é carregado do

disco para a memória, esse passa a ser denominado processo. Um ponto importante que deve ser considerado ao carregar um processo na memória é a quantidade de memória que deve ser alocada. Se processos são criados com um tamanho fixo, inalterável, ou seja, o sistema operacional alocará exatamente aquilo o que é necessário, então a alocação é simples. Contudo, se a área de dados do processo puder crescer, como a alocação dinâmica de memória em uma área temporária (*heap*), assim como ocorre em muitas linguagens de programação, então, problemas poderão ocorrer sempre que um processo tentar crescer. Caso haja espaço livre disponível adjacente ao processo, ele poderá ser alocado e o processo poderá crescer nesse espaço. Por outro lado, se estiver adjacente a outro processo, o processo que necessita crescer poderá ser movido para uma área de memória grande, o suficiente para contê-lo, dessa forma, um ou mais processos terão que ser transferidos para o disco a fim de criar essa área disponível.

Como o esperado é que a maioria dos processos cresça durante a execução, então é alocada uma memória extra sempre que se fizer a transferência de um processo para a memória ou a movimentação dele na memória. Assim, dentro do espaço de endereçamento de cada processo pode conter duas áreas em expansão: a área de dados usada como área temporária (*heap*) para variáveis dinamicamente alocadas e liberadas, e uma área de pilha para variáveis locais e para endereços de retorno (*stack*). Na Figura 33, é mostrado que cada processo tem uma pilha no topo de sua memória alocada, que cresce para baixo, e uma área de dados adjacente ao código do programa, que cresce para cima. A porção da memória situada entre as duas áreas pode ser usada por ambas [42].

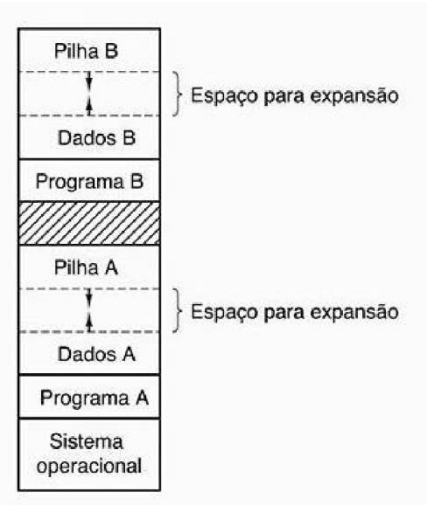


Figura 33 - Alocação de espaço de uma pilha e um segmento de dados em crescimento. Retirada de [42].

De maneira análoga, a heurística IDS considera que o espectro seja divido em dois segmentos e cada segmento contém uma estrutura de pilha que cresce em direção ao centro do espectro. O primeiro segmento tem a base da pilha posicionada na extremidade superior e o segundo na extremidade inferior formando duas pilhas invertidas. Dessa maneira, ao utilizar o algoritmo FF podem-se definir duas direções de alocação: ordem direta e ordem inversa. As alocações, qualquer que seja a ordem, são realizadas sequencialmente e crescem uma em direção à outra, assim como ocorre dentro dos espaços de endereçamento dos processos como mostrado na Figura 34.

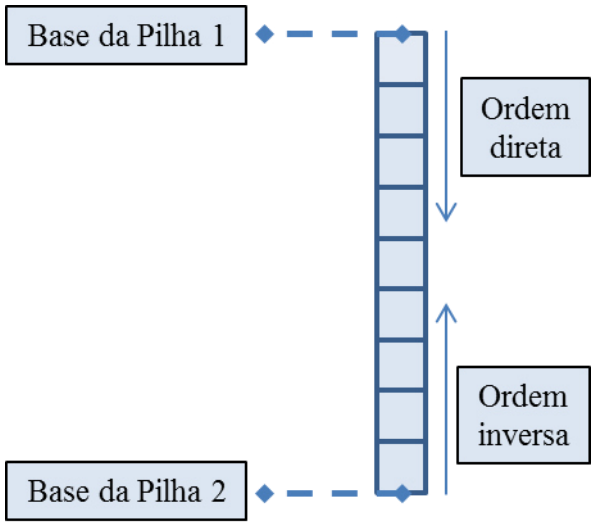


Figura 34 - Funcionamento da heurística IDS.

A expressão da heurística IDS é dada por (3), e as condições 1 e 2 representam a política utilizada. Nessa proposta, utiliza-se a política de tráfego compartilhado em que a condição 1 verifica se o bloco de alocação é do caminho primário, e a condição 2 verifica se o bloco de alocação é do caminho de proteção compartilhada.

$$\text{alocação}_{\text{IDS}}(\text{num}_{\text{fsus}}) = \begin{cases} first\_fit\_\text{direto}(\text{num}_{\text{fsus}}), & \text{Se condição 1} \\ first\_fit\ \_\text{inverso}(\text{num}_{\text{fsus}}), & \text{Se condição 2} \end{cases} \quad (3)$$

A heurística IDS com a política de tráfego compartilhado possui uma sinergia com a implementação do SPP ASP. No SPP ASP a restrição de compatibilidade de largura de banda é eliminada permitindo que a banda se intercale e os recursos sejam compartilhados individualmente (Seção 3.3.1), dessa forma a heurística IDS aumenta o número de compartilhamento concentrando os blocos de alocação compartilhados em uma das extremidades da pilha de alocação. A Figura 36 e Figura 37 mostram esse contraste ao efetuar

a mesma sequência de alocação. Na Fig.35a até Fig.35d os FSUs são alocados sequencialmente, intercalando caminhos (P)rimários e (S)ecundários compartilhados, no sentido direto.

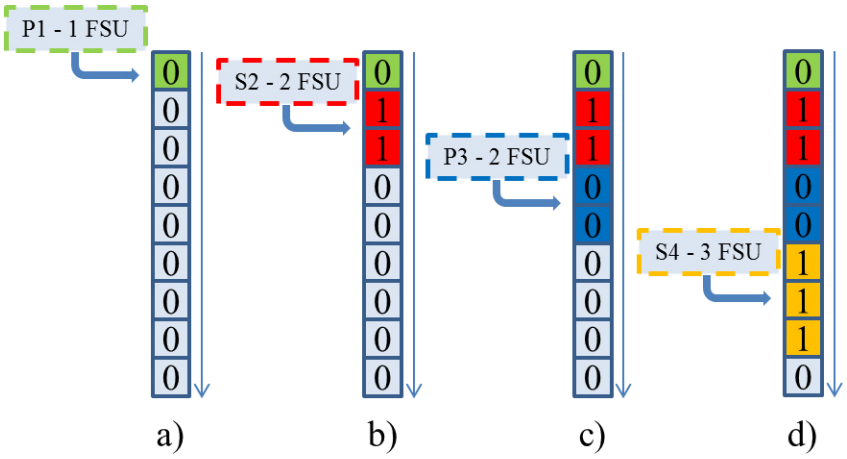


Figura 35 - Alocação de caminhos (P)rimários e (S)ecundários com SPP ASP.

Por outro lado, nas Fig.36a e Fig.36c os espectros dos caminhos primários são alocados na primeira pilha um após o outro no sentido direto e nas Fig.36b e Fig.36d os espectros dos caminhos secundários são alocados e compartilhados na segunda pilha no sentido inverso. Os principais efeitos observados na Fig.36d em relação a heurística IDS são:

1) Aumenta o número de compartilhamentos nas posições mais próximas da base da segunda pilha de alocação;
2) Permite economizar recursos, que possibilita o atendimento de mais demanda de tráfego.

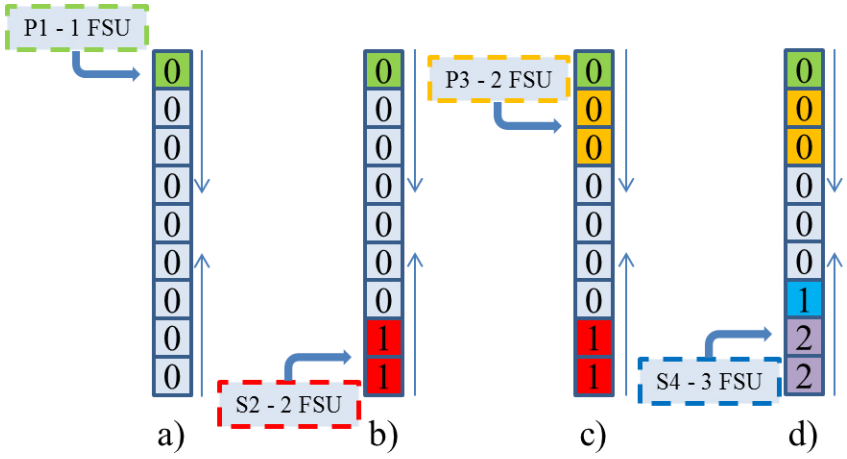


Figura 36- Alocação de caminhos (P)rimários e (S)ecundários com SPP ASP IDS.

5 SIMULAÇÃO

A proposta deste trabalho é estudar algoritmos RSA com proteção e restauração, especificamente os trabalhos realizados por Chen *et al.* [8] e por Sone *et al.* [10]. Pretende-se também utilizar a heurística de alocação IDS para avaliar a sua contribuição em relação às demais heurísticas.

Primeiramente, foi desenvolvido um modelo de simulação que é dividido em três partes: modelo de rede, modelo do plano de controle e modelo de geração de tráfego e de falhas. Em seguida apresentam-se as métricas utilizadas na simulação e a formulação do problema. O experimento simula um algoritmo RSA que utiliza esquemas de proteção DPP e SPP, sendo que este último conta com a utilização de heurísticas adicionais como o DLBSPP e o IDS, e esquemas de restauração TAR e BSR. Esse conjunto de esquemas de proteção e restauração e heurísticas serão agrupados de acordo com alguns critérios de comparação.

5.1 Modelagem da Simulação

Uma simulação é um conjunto de operações lógicas e matemáticas as quais permitem imitar o funcionamento de um sistema ou processo do mundo real. O comportamento do sistema é estudado pela construção de um modelo de simulação que normalmente toma a forma de um conjunto de considerações relacionadas à sua operação. Estas considerações são expressas por meio de relações matemáticas, lógicas e simbólicas entre as entidades do sistema. Um sistema é definido como um grupo de objetos que estão interligados de alguma forma, para a realização de algum objetivo. Os componentes de um sistema são [43]:

1) Entidade: objeto de interesse no sistema;
2) Atributo: uma propriedade de uma entidade;
3) Estado do sistema: a coleção de variáveis necessárias para descrever o sistema em um dado instante;
4) Atividade: uma ação que para ser realizada consome certa quantidade de tempo;
5) Evento: uma ocorrência instantânea que pode mudar o estado do sistema;

Nessa simulação, o modelo é dividido em três partes: modelo de rede, modelo do plano de controle e modelo de geração de tráfego e de falhas.

5.1.1 Modelo de rede

O modelo de rede é uma representação abstrata dos componentes da rede e de seus recursos de modo que o seu funcionamento possa ser modelado por operações lógicas e matemáticas. O que caracteriza o modelo de rede é a arquitetura de rede que ele está representando, neste caso uma EON. As entidades do modelo de rede são concebidas sob dois pontos de vista: elementos de topologia e elementos de recurso (banda). Os elementos de topologias são representados pelas entidades *nó* e *enlace*, cujas interconexões formam um grafo como descrito na Seção 4.1. O elemento de recurso é representado pela entidade FSU, como descrito na Seção 4.2. Essas entidades descrevem os componentes da arquitetura da rede e mantêm-se inalteradas durante toda a simulação e, por isso, são chamadas entidades permanentes. Outra entidade considerada no modelo de rede é a *conexão*, que é uma entidade temporária, pois ela é criada e removida durante a simulação. A *conexão* representa o atendimento de uma requisição de banda de um cliente, ou seja, é o serviço prestado pela rede. A Tabela 5 relaciona as principais entidades do modelo de rede e em seguida são apresentados os seus principais atributos.

Tabela 5 - Entidades principais do modelo de rede

Entidade	**Tipo**
Nó	Permanente
Enlace	Permanente
FSU	Permanente
Conexão	Temporária

Os principais atributos do *nó* são mostrados na Figura 37. O identificador é um número inteiro positivo sequencial que é utilizado para indexar o nó correspondente na representação da rede, seja por lista de adjacência ou por matriz de adjacência. As listas de portas de entrada e saída correspondem às interligações com os enlaces que entram e saem do nó. As portas de saída de cada *nó* correspondem (parcialmente) à representação por lista de adjacência.

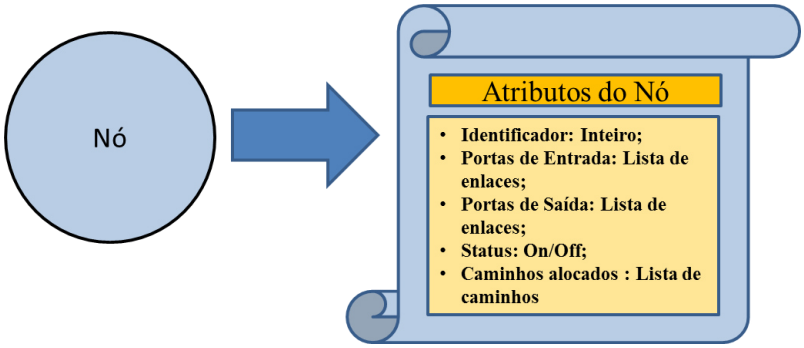


Figura 37 - Atributos da entidade Nó.

Os dois últimos atributos do *nó* são reservados para lidar com as falhas. O atributo "s*tatus*" é uma *flag* que indica o funcionamento do *nó*, ou seja, indica se o *nó* está operando normalmente ou se ocorreu uma falha. O atributo "caminhos alocados" é um registro de controle que mantém a lista de todos os caminhos (primários e secundários) alocados que passam pelo *nó*. Esse registro de controle é importante para que na ocorrência de uma falha no *nó*, as informações dos caminhos alocados nele sejam obtidas de maneira rápida e direta.

Os atributos da entidade *enlace* são mostrados na Figura 38. Um *enlace* possui duas extremidades de ligação, os nós interligados por ele são indicados pelos atributos "nó fonte" e "nó destino". O atributo "comprimento" é o comprimento espacial do enlace que denota a distância de transmissão do sinal e que pode também ser utilizado como o custo de cada salto computado pelos algoritmos de roteamento. Em seguida, o atributo "espectro" representa o conjunto de subportadoras que compõe a banda. Nas EONs, cada subportadora é manipulada individualmente e, por isso, cada subportadora é uma instância da entidade FSU. Detalhes sobre o FSU será explicado mais adiante.

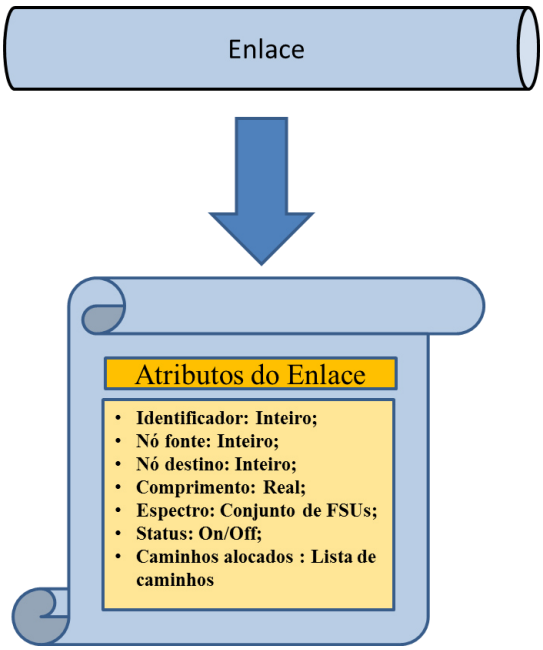


Figura 38 - Entidade Enlace e seus atributos.

Da mesma forma que o *nó*, o *enlace* também contém atributos que lidam com as falhas. O atributo "s*tatus*" é uma *flag* que indica o funcionando do enlace e "caminhos alocados" é o registro de controle que contém a lista de todos os caminhos (primários e secundários) que passam por ele. Esses atributos estão contidos tanto no *nó* como no *enlace* porque ambas as entidades podem falhar e, assim, o modelo de rede proposto permite uma simulação que trate tanto de falhas ocorridas nos nós quanto nos enlaces.

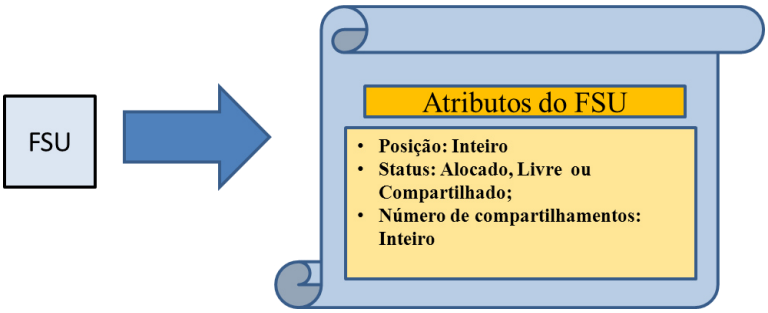


Figura 39 - Entidade FSU e seus atributos.

O atributo "espectro" do *enlace* corresponde à banda óptica de transmissão e é representada por um conjunto de FSUs. O FSU, mostrado na Figura 39, é a entidade que representa a mínima granularidade de banda. No atendimento de uma conexão, um conjunto consecutivo de FSUs pode ser alocado de forma concatenada para formar o canal de tamanho arbitrário, permitindo inclusive a formação dos supercanais ópticos (ver Seção 2.1). Nas EONs, cada FSU pode ser manipulada individualmente pelo plano de controle, por exemplo:

seleção de formatos de modulação, compartilhamento de recursos. O modelo de rede proposto visa simular o desempenho dos algoritmos RSA envolvendo proteção e restauração, por isso os principais atributos definidos para esta entidade referem-se ao compartilhamento de recursos, como abordado na Seção 3.3.1. O primeiro atributo indica a posição do FSU no espectro e serve para identificá-lo. O segundo atributo, "Status", pode ser de três tipos: alocado, livre e compartilhado. No caso de um FSU compartilhado, considera-se então um terceiro atributo: "número de compartilhamentos", que registra o número de vezes que o FSU foi compartilhado. Este último é utilizado pelo plano de controle para definir o máximo de compartilhamentos e também permitir liberar o recurso de maneira consistente, impedindo que uma proteção compartilhada seja liberada deixando outros caminhos primários correspondentes desprotegidos.

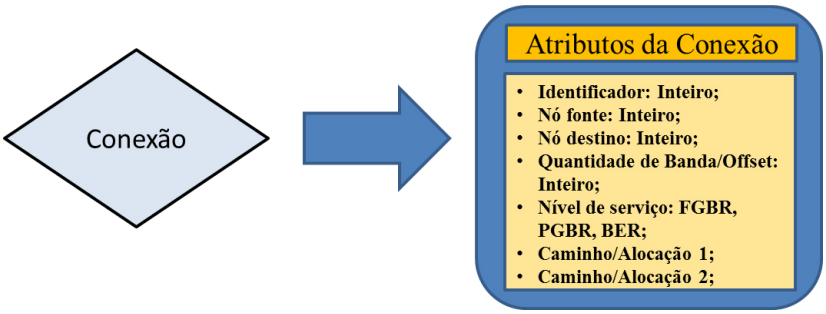


Figura 40 - Entidade Conexão e seus atributos.

Quando uma demanda de conexão é atendida pela rede, uma quantidade de FSUs é alocada nos enlaces da rota que compreende os nós fonte e destino. As informações associadas a esses blocos de alocação são guardadas em outra entidade chamada *conexão* (Figura 40). A *conexão* é uma entidade temporária que é criada no momento do estabelecimento da conexão de rede, ou seja, quando os FSUs dos enlaces da rota são alocados, e é excluída quando termina o seu tempo de duração. O primeiro atributo da *conexão* é o "identificador", responsável por associar a conexão alocada com os seus respectivos eventos de chegada e partida (ver Seção 5.1.2). Os atributos "nó fonte", "nó inicial", "quantidade de banda/offset" e "nível de serviço" são as informações da demanda de conexão, que são utilizadas como parâmetros pelos algoritmos RSA para resolver os caminhos e alocações primários e secundários representados respectivamente pelos atributos "caminho/alocação 1" e caminho/alocação 2". O conjunto de conexões estabelecidas na rede em determinado instante representa o estado da rede naquele instante. O atributo "nível de

serviço" tem utilidade apenas para computação dos caminhos secundários ou de proteção segundo o esquema BSR descrito na Seção 3.5.

As entidades acima descritas são os componentes do modelo utilizados para criar uma representação genérica de uma EON. O primeiro passo é a construção da topologia, que consiste em interligar os nós e enlaces da rede. A principal restrição para a construção da topologia de rede é que o enlace não contenha "pontas soltas", ou seja, as duas extremidades do enlace precisam ser interligadas com dois nós quaisquer. As seguintes ações são tomadas:

1. Para cada *enlace* escolha dois nós e atribua o "nó fonte" e o "nó destino", assumindo que a direção de transmissão seja do nó fonte para o nó destino;
2. Adicione no *nó* fonte o enlace atual na lista de portas de saída;
3. Adicione no *nó* destino o enlace atual na lista de portas de entrada.

Esse processo é realizado sistematicamente na construção da topologia de rede para cada enlace que interliga dois nós. A Figura 41 mostra uma rede parcialmente construída em que os enlaces 1 e 2 contém "pontas soltas" (precisam ser interligadas) e um par de enlaces 3 e 4 que representa uma transmissão bidirecional entre os nós 1 e 2. As flechas pontilhadas indicam a direção de transmissão em cada enlace.

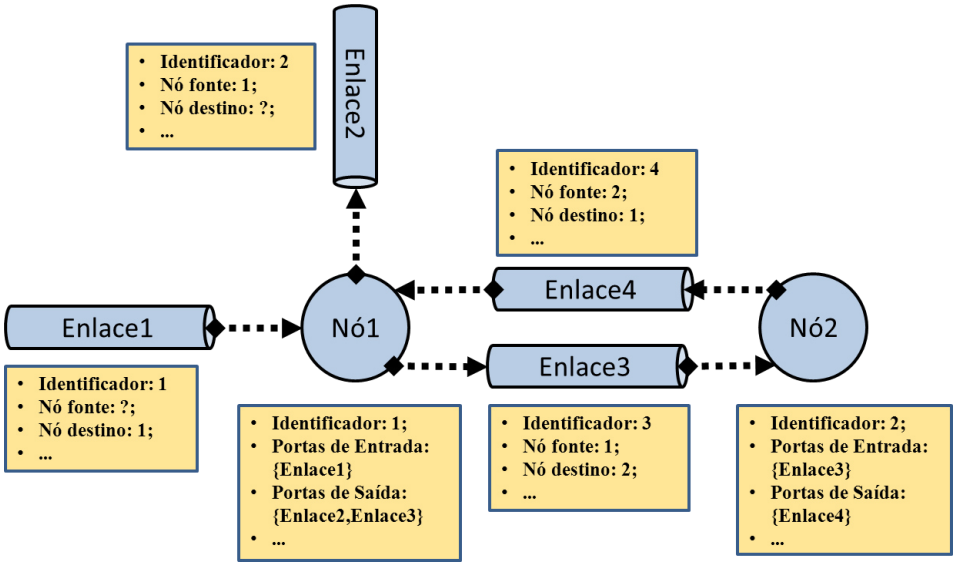


Figura 41 - Interligações entre Nós e Enlaces.

Depois de criada uma topologia, o próximo passo é a criação do conjunto de FSUs que compõe a banda em cada enlace. A quantidade de recursos nos enlaces da rede pode ser homogênea, iguais para todos os enlaces, ou heterogênea, quantidades diferentes nos enlaces da rede. Um exemplo de composição de FSUs em um enlace é mostrado na Figura 42.

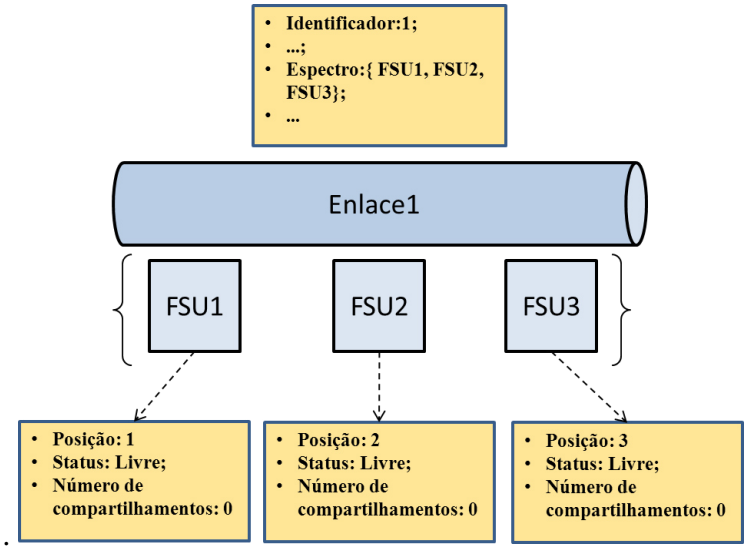


Figura 42 - Banda do enlace composta de FSUs.

Uma vez construída a topologia e os recursos de banda, os demais parâmetros da rede precisam ser inicializados. A Figura 43 mostra os atributos de uma unidade mínima de rede contendo 2 nós e 1 enlace unidirecional no seu estado inicial de operação. Esse estado ocorre antes de iniciar uma simulação e após o seu término quando todas as conexões são liberadas.

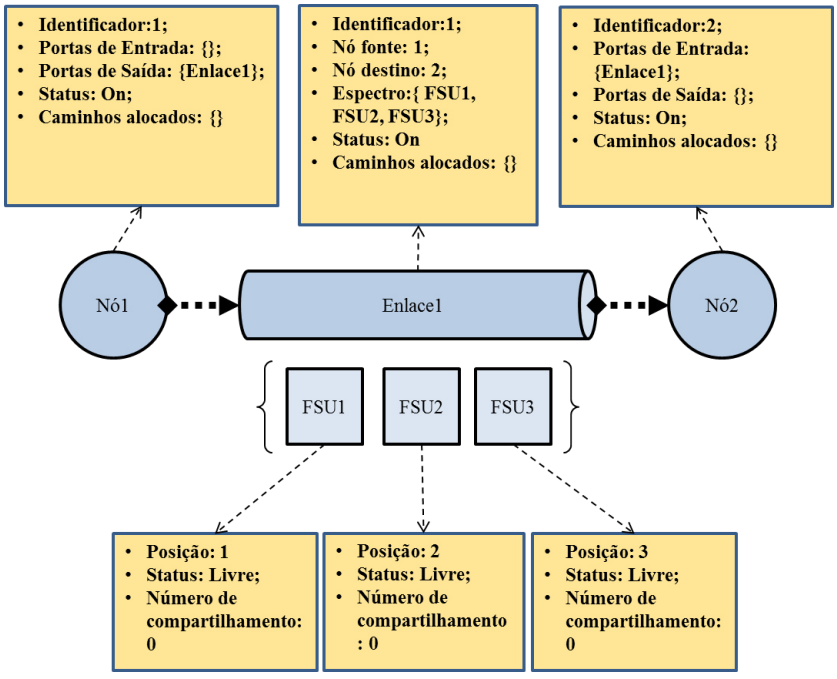


Figura 43 - Estado inicial de uma unidade de rede (2 Nós, 1 Enlace).

Os estados intermediários da configuração apresentada na Figura 43 correspondem aos estados de alocação das conexões de entrada. Adota-se uma entrada de conexão entre os enlaces 1 e 2 com uma demanda de banda de 2 FSUs. A solução RSA apresentada é o

caminho (1,2) e as alocações (1,2). A Figura 44 mostra o estado de alocação da rede após o estabelecimento dessa conexão. O processo de estabelecimento da conexão é apresentado a seguir na Seção 5.1.2, que compõe as regras do modelo do plano de controle.

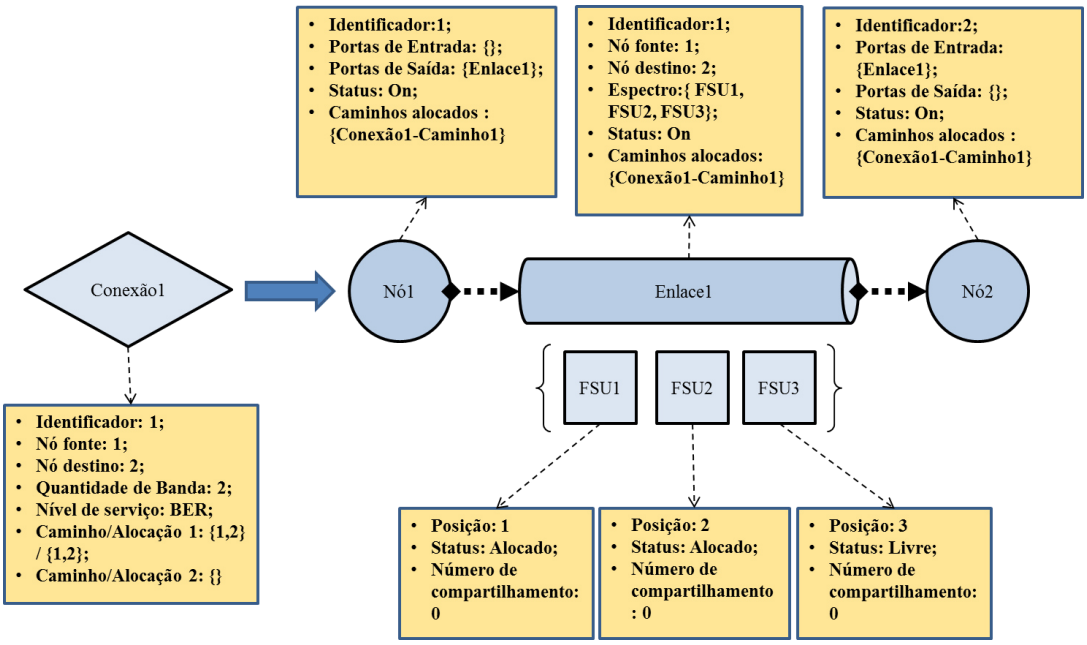


Figura 44 - Estado da unidade de rede após um atendimento de Conexão (Alocação da demanda).

5.1.2 Modelo do plano de controle

O modelo do plano de controle é a abstração do conjunto de ações e tomadas de decisão para cada evento do sistema. As ações são as atividades da simulação, os quais levam certo tempo para serem realizadas e podem alterar o estado da rede. O funcionamento da rede baseia-se na chegada e atendimento de conexões, portanto dois eventos principais são considerados: chegada de conexão e partida de conexão. Tais eventos são chamados de eventos endógenos, pois fazem parte do funcionamento do sistema. Dois outros eventos também são considerados nesse trabalho, o evento de ocorrência de falha e o evento de reparação de falha. Esses últimos são chamados de eventos exógenos, que são eventos externos ao sistema, mas que afetam o seu funcionamento. A Tabela 6 mostra os eventos do sistema considerados pelo plano de controle.

Tabela 6 - Tipos de Eventos

Eventos	Tipo
Chegada de Conexão	Endógeno
Partida de Conexão	Endógeno
Ocorrência de Falha	Exógeno
Reparação da Falha	Exógeno

Os eventos principais são: eventos de conexão e eventos de falha. O tipo evento de conexão é subdividido em dois subeventos: de chegada de conexão, que traça o caminho e reserva os recursos, e de partida de conexão, que libera recursos de rede ao longo da rota estabelecida. De maneira similar, o evento de falha é subdividido em dois subeventos: o evento de ocorrência de falha em um enlace, que inutiliza um enlace da rede atribuindo-lhe um custo infinito, e o evento de reparação da falha, que retorna o custo original do enlace da falha.

O evento é representado por uma estrutura de dados como apresentado na Figura 45. O primeiro atributo "tempo" é a chave de ordenação que sequencia os eventos discretos de acordo com alguma função de distribuição. A função de distribuição será explicada na Seção 5.1.3. Os demais atributos possuem significados diferentes para cada tipo de evento e são mostrados na Tabela 7.

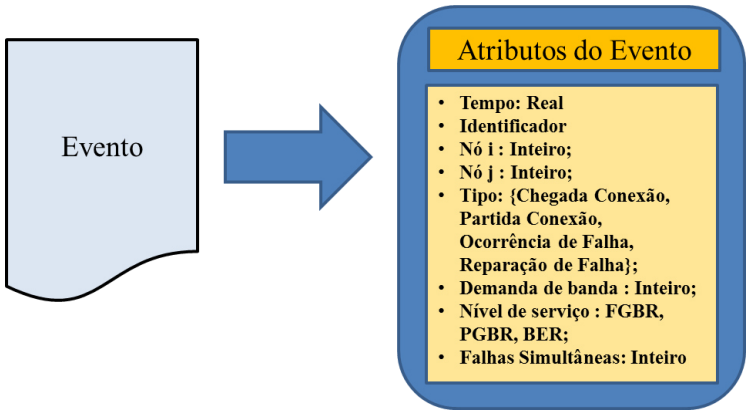


Figura 45 - Evento e seus atributos.

Tabela 7 - Significado dos atributos para cada tipo de evento.

Evento	Atributo	Descrição
Chegada de conexão	Tempo	Tempo da chegada de conexão
	Identificador	Corresponde o identificador da conexão
	No i:	Nó fonte
	Nó j	Nó destino
	Demanda de banda	Banda requerida
	Nível de serviço	O tipo de proteção caso seja utilizado BSR
Partida de conexão	Tempo	Tempo da partida da conexão
	Identificador	Corresponde o identificador da conexão
	Nó i:	Nó fonte
	Nó j	Nó destino
	Demanda de banda	Banda requerida
	Nível de serviço	O tipo de proteção caso seja utilizado BSR
Ocorrência de falha	Tempo	Tempo da ocorrência de falha
	Identificador	Não utilizado
	Nó i:	Nó anterior ao enlace da falha
	Nó j	Nó posterior ao enlace da falha
	Demanda de banda	Não utilizado
	Nível de serviço	Não utilizado
Reparação de falha	Tempo	Tempo da restauração de falha
	Identificador	Não utilizado
	Nó i:	Nó anterior ao enlace a ser restaurado
	Nó j	Nó posterior ao enlace a ser restaurado
	Demanda de banda	Não utilizado
	Nível de serviço	Não utilizado

A sequência de ações/atividades realizadas após cada evento faz parte da abstração do modelo do plano de controle e o seu funcionamento segue as mesmas instruções apresentadas na Seção 2.4. A seguir, apresentam-se os detalhes sobre a sequência de atividades que são desencadeadas após cada evento do sistema. As atividades serão representadas por diagramas

de fluxo em que os blocos de cor laranja representam funcionalidades de roteamento e blocos de cor verde representam as funcionalidades de sinalização.

Quando o evento é de chegada de conexão (Figura 46) a primeira atividade é a execução do algoritmo RSA que encontra uma solução para o caminho primário. Nesse modelo, assume-se que a topologia e estado dos recursos da rede sejam previamente conhecidos e atualizados no instante do evento, ou seja, corresponde ao modelo de gerenciamento centralizado. Se o algoritmo não encontrar uma solução, então a conexão de entrada é bloqueada, senão o algoritmo é executado novamente para encontrar o caminho secundário disjunto do primário. Se não for possível encontrar um caminho secundário a conexão também é bloqueada. A conexão será estabelecida se e somente se o roteamento encontrar solução para o caminho primário e para o caminho secundário. O estabelecimento da conexão é uma sinalização propagada em todos os enlaces das rotas e realiza as respectivas reservas de recursos.

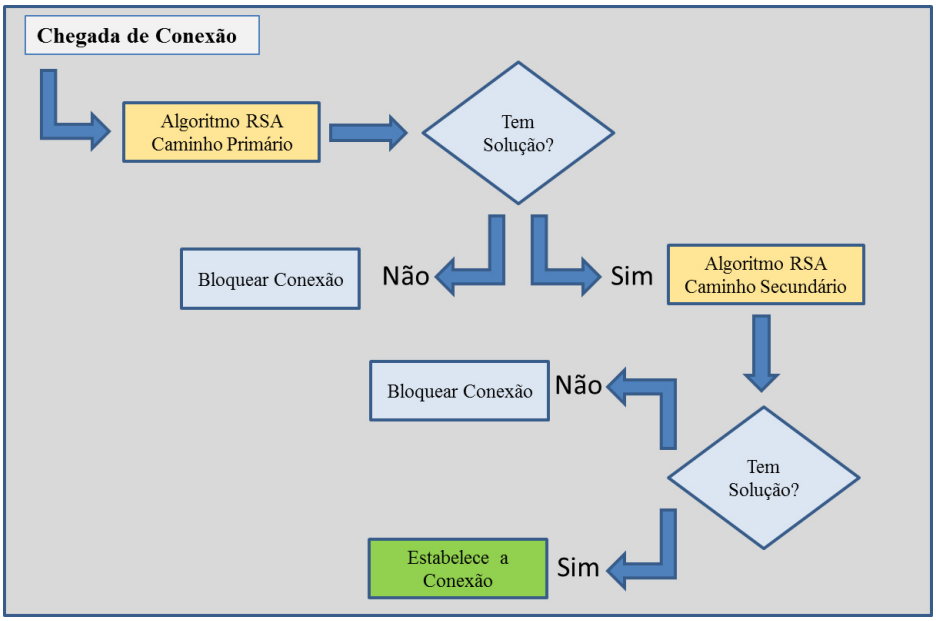


Figura 46 - Fluxo de atividades para o evento de chegada de conexão.

Para cada evento de chegada de conexão é gerado um evento de partida de conexão. Quando um evento de partida de conexão é acionado, não existem garantias de que a sua respectiva conexão tenha sido estabelecida anteriormente, pois ela pode ter sido bloqueada. Por esse motivo, primeiramente efetua-se uma busca entre as conexões ativas utilizando o "identificador" como chave de busca. Caso exista uma conexão ativa, a única operação realizada nesse tipo de evento é a sinalização de remoção da conexão, que libera os recursos

por todos os enlaces das rotas estabelecidas pelos caminhos primário e secundário, conforme mostrado na Figura 47.

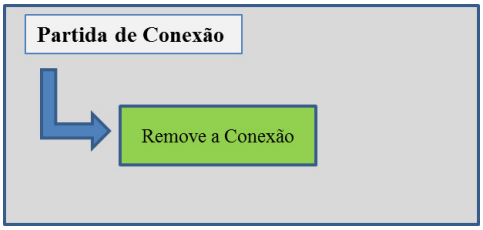


Figura 47 - Fluxo de atividades para o evento partida de conexão.

Uma falha de rede é representada pelo evento de ocorrência de falha que desencadeia o fluxo da Figura 48. Quando esse evento é acionado o custo do enlace da falha é definido com o valor infinito e o seu "status" é alterado para "off". Uma falha em um ou mais enlaces de rede provoca a interrupção de inúmeros caminhos de conexão. No instante seguinte à falha inicia-se o processo de restauração para todas as conexões ativas que passam pelo enlace da falha. Para cada conexão ativa (caminho primário/caminho de trabalho) verifica-se se existe proteção disponível, ou seja, se existe um caminho secundário que não foi afetado por alguma falha e que possa ser utilizado. Caso exista, a comutação do fluxo de dados é sinalizada para este caminho de proteção e ele se torna o caminho de trabalho. Uma vez que a conexão tenha comutado o seu caminho de trabalho para o caminho secundário ela fica sem proteção, pois não foi considerado o reestabelecimento de uma nova proteção após a comutação de caminho. Caso não exista proteção disponível, a restauração dinâmica por meio do algoritmo de RSA pode ser executada na tentativa de encontrar outro caminho de trabalho para o restabelecimento da conexão. Se outro caminho for encontrado então ele é alocado e a conexão reestabelecida, senão ela é removida e todos os seus recursos liberados. O fluxo de atividades representado na Figura 49 mostra o processo mais completo de restauração. Em alguns casos da simulação, a restauração dinâmica não será acionada e, assim, é possível medir apenas a capacidade de recuperação das conexões por meio da comutação de caminhos de proteção.

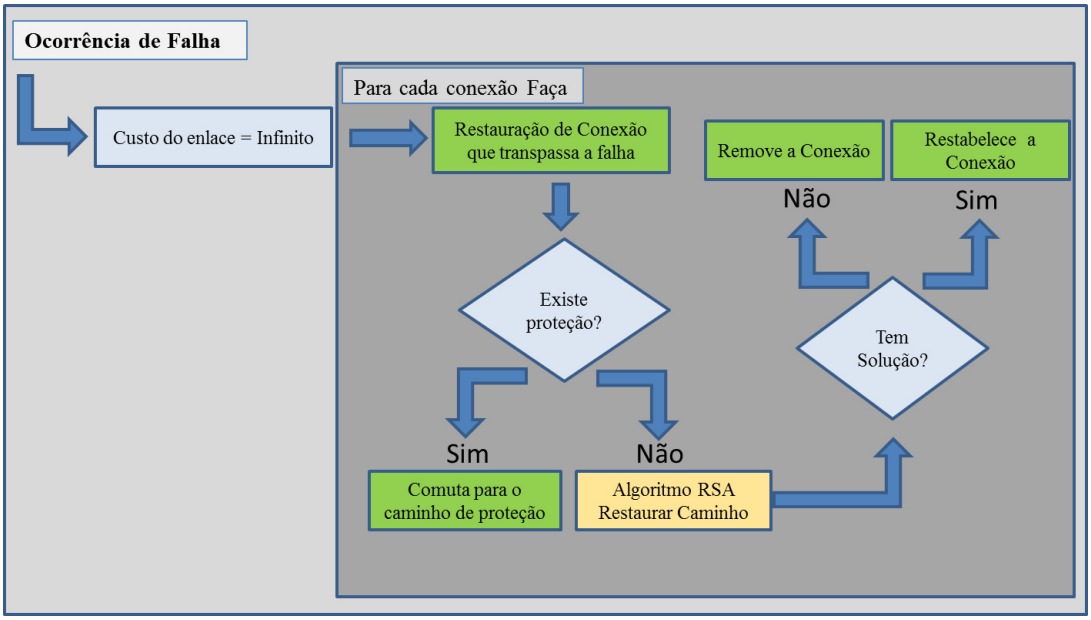


Figura 48 - Fluxo de atividades para o evento de ocorrência de falha.

Para cada evento de ocorrência de falha é criado um evento de reparação de falha que reestabelece o funcionamento do enlace da falha atribuindo o seu custo original e habilitando o seu *status* para "on" como mostrado na Figura 49.

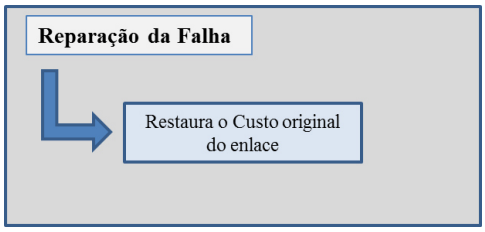


Figura 49 - Fluxo de atividades para o evento de restauração de falha.

5.1.3 Modelo de geração de tráfego e de falhas

Em um sistema de telecomunicações a modelagem da simulação discreta baseia-se na chegada e atendimento das conexões. Uma modelagem desse tipo segue as características de um sistema de filas. Para caracterizar um sistema de filas, é necessário identificar as propriedades probabilísticas do fluxo de entrada de conexões, os tempos de serviço e disciplinas de serviço.

Em teoria de filas, os tempos entre chegadas são geralmente variáveis aleatórias independentes e identicamente distribuídas. Outra variável aleatória é o tempo de conexão, às vezes chamado de solicitação de serviço ou de trabalho, que também são comumente consideradas variáveis aleatórias independentes. Seja P uma função de probabilidade. A

probabilidade que ocorra uma chegada de conexão até o tempo t é denotado por (4). Analogamente, a probabilidade que uma conexão permaneça em atendimento até um tempo x é denotado por (5),

$$A(t) = P(tempo\ entre\ chegadas < t) \quad (4)$$

$$B(x) = P(tempo\ de\ serviço < x) \quad (5)$$

Outras características de um sistema de fila é a estrutura do serviço e a disciplina do serviço. A estrutura do serviço nos diz o número de servidores e a capacidade do sistema, que é o número máximo de clientes que permanecem no sistema, incluindo as que estão sendo atendidos. A disciplina de serviço determina a regra de acordo como o próximo cliente é selecionado. As regras mais comumente utilizadas são [44]:

1) First in first out (FIFO);
2) Last in first out (LIFO);
3) Random service (RS);
4) Prioridade.

Primeiramente, para simplificar, considera-se um sistema com um único servidor. Seja ϱ, denominada intensidade de tráfego, é definida por:

$$\varrho = \frac{tempo\ médio\ de\ serviço}{tempo\ médio\ entre\ chegadas} \quad (6)$$

Assumindo um sistema de população infinita com intensidade de chegada λ, o tempo médio entre chegadas é $1/\lambda$ e a taxa média de atendimento denotada por μ, então o tempo médio de serviço é $1/\mu$. Assim, a intensidade de tráfego é:

$$\varrho = intensidade\ de\ chegada\ .tempo\ médio\ de\ serviço = \frac{\lambda}{\mu} \quad (7)$$

O parâmetro intensidade de tráfego é uma unidade adimensional medida em *erlang*. O nome desta unidade se deve ao matemático e engenheiro dinamarquês Agner Krarup Erlang, que introduziu os estudos de teoria de filas para solucionar problemas de congestionamento em redes de telefonia no início do século XX [44].

No caso da simulação proposta, suponha-se que tanto a chegada de conexões quanto o tempo de atendimento sejam variáveis aleatórias exponencialmente distribuídas; que o número de linhas de serviço seja "c" e que a capacidade do sistema ou o número máximo de usuários na fila também seja "c". Esse tipo de sistema de fila, usando a notação de Kendall, é denotado por M/M/c/c. Em resumo, tem-se um sistema com as seguintes características [45]:

1) O processo de chegada de conexões segue uma distribuição de Poisson com parâmetro λ_c (processo Markoviano);
2) O processo de tempo de serviço segue uma distribuição exponencial negativa com parâmetro μ_c (processo Markoviano);
3) O número máximo de linhas é *c* (No caso de demandas de banda com a mínima granularidade);
4) A capacidade também é *c* (Número total de FSUs).

O processo de Poisson é um dos mais importantes processos aleatórios em teoria das probabilidades. Ele é amplamente utilizado para modelar pontos aleatórios no tempo e no espaço, como os tempos de emissões radioativas, os tempos de chegada dos clientes em um centro de serviço, e modelagem de tráfego em redes de telecomunicações. Várias distribuições de probabilidade importantes surgem naturalmente do processo de Poisson: a distribuição de Poisson e a distribuição exponencial. Uma característica importante do processo de Poisson é que os tempos entre as chegadas são independentes.

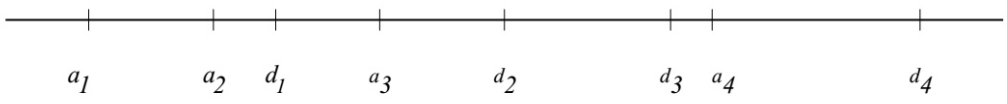


Figura 50: Chegada e partida das conexões [45].

A Figura 50 mostra um caso discreto para a chegada e partida de quatro conexões. As chegadas são marcadas nos tempos $a_1, a_2, a_3 \, e \, a_4$ e são liberadas respectivamente nos tempos $d_1, d_2, d_3 \, e \, d_4$. Os intervalos entre chegadas são $I_i = a_{i+1} - a_i$. Os intervalos $S_1 = d_1 - a_1$, $S_2 = d_2 - d_1$, $S_3 = d_3 - d_2$ e $S_4 = d_4 - a_4$ são chamados tempos de serviço ou tempos de atendimento.

A probabilidade para que uma chegada até o tempo t, denotado por A(t), para conexão de número n, é dada pela distribuição de Poisson:

$$P_r(A(t) = n) = e^{\lambda t}\frac{(\lambda t)^n}{n!} \quad (8)$$

A probabilidade para que uma primeira chegada A_1 ocorra depois do tempo t é

$$P_r(A(t) = 0) = e^{\lambda t}\frac{(\lambda t)^0}{0!} = e^{\lambda t} \quad (9)$$

Note que os seguintes eventos são complementares, pois apenas um deles ocorre:

1) O tempo de espera t para no mínimo uma chegada dentro do intervalo [0, t];
2) Nenhuma chegada intervalo de [0, t].

Assim, a probabilidade de ocorrer uma chegada até o tempo t é dado por

$$P_r(A_1 \leq t) = 1 - e^{-\lambda t} \quad (10)$$

Como os tempos de chegada de conexão são incrementos estacionários, ou seja, que a distribuição de probabilidade de qualquer incremento A(t) – A(s) depende apenas do comprimento t - s do intervalo de tempo, os intervalos de tempo entre chegadas de quaisquer dois eventos subsequentes seguem a mesma distribuição. Dessa forma, como mostrado no exemplo da Figura 50, os intervalos entre chegadas das conexões I_c podem ser expressos por (11). Da mesma maneira, os tempos de serviço das conexões S_c são expressos por (12). As funções dadas por (11) e (12) compõem a base matemática do modelo de geração de tráfego adotado na simulação,

$$P_{ri}(I_c < t) = 1 - e^{-\lambda t} \quad (11)$$

$$P_{rs}(S_c < x) = 1 - e^{-\mu x} \quad (12)$$

O cálculo dos tempos entre chegadas de conexão e os tempos de serviço podem ser realizado diretamente por (13) e (14) em que o valor de "*rand*" é um número aleatório distribuído uniformemente no intervalo [0,1) e os parâmetros λ_c e μ_c são, respectivamente, a taxa média de entre chegadas de conexão e o taxa média de serviço de conexão,

$$\mathrm{I}_c = \frac{\ln(1-rand)}{\lambda_c} \quad (13)$$

$$S_c = \frac{\ln(1-rand)}{\mu_c} \quad (14)$$

Assim, o tempo de chegada de uma nova conexão é calculado (15) e seu tempo de partida é dado por (16),

$$t_{a+1} = t_a + I_a \quad (15)$$

$$t_d = t_{a+1} + S_a \quad (16)$$

A Figura 51 apresenta o diagrama de fluxo para a criação dos tempos dos eventos de conexão. Primeiramente, inicializa-se a variável acumulativa de tempo $t_a = 0$ e o contador de conexões $\mathrm{ID\_C} = 0$. Para cada conexão calcula-se (13) e (14), depois se calcula (15) e em seguida (16). Os tempos t_a e t_d obtidos são atribuídos aos eventos de chegada de conexão e partida de conexão, respectivamente. Quando todos os eventos de conexões tiverem sido gerados o conjunto de eventos é ordenado em ordem crescente utilizando o atributo "tempo" como chave de ordenação.

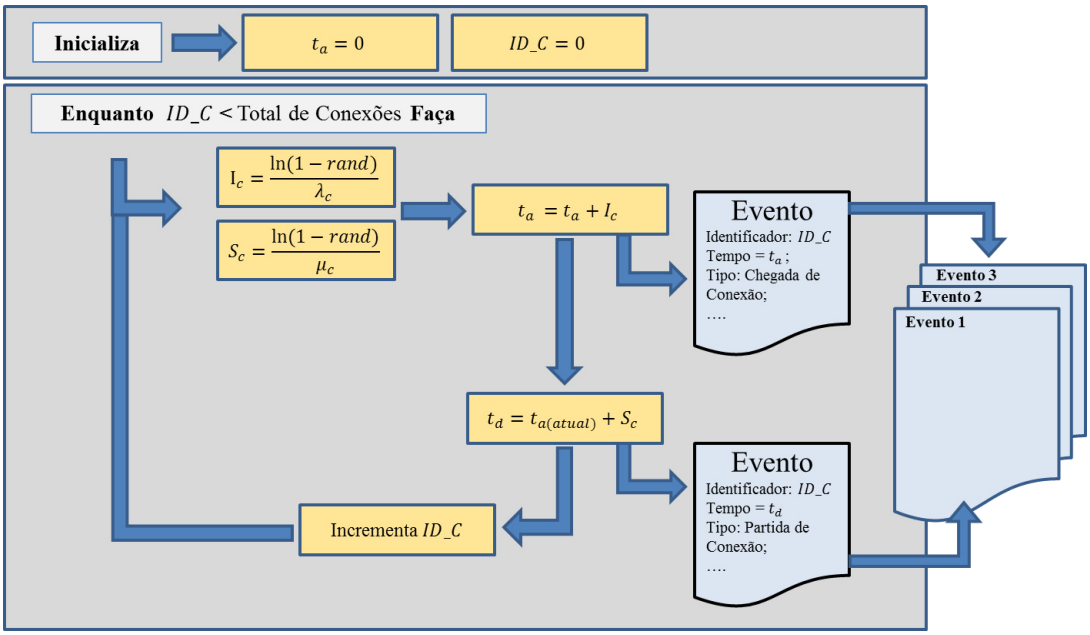


Figura 51 - Diagrama simplificado de geração de eventos de chegada e partida de conexão

Quanto ao modelo de geração de falhas utiliza-se distribuição uniforme com tempos de manutenção da falha muito menor do que o intervalo entre ocorrência de falhas. Esse

modelo foi escolhido para garantir que cada falha não ocorra antes da falha anterior ter sido restaurada. Assim, podem-se criar janelas de falhas em que não intercalem. Os tempos entre ocorrências de falha e os tempos de permanência de falha são constantes calculados diretamente por (17) e (18) em que os parâmetros λ_f e μ_f são, respectivamente, a taxa média de entre ocorrência de falha e a taxa média de manutenção de falha,

$$\mathrm{I}_f = \frac{1}{\lambda_f} \quad (17)$$

$$S_f = \frac{1}{\mu_r} \quad (18)$$

Os tempos de ocorrência de falha e reparação de falha de cada novo evento de falha são calculados, respectivamente, por:

$$t_{f+1} = t_a + I_a \quad (19)$$

$$t_r = t_{f+1} + S_f \quad (20)$$

Ambos os modelos são caracterizados pelos parâmetros λ_c, μ_c, λ_f e μ_f, porém, as suas inicializações são feitas de formas diferentes. Para o modelo de geração de tráfego o tempo inicial do atendimento das conexões é $t_a = 0$ e os parâmetros λ_c e μ_c são obtidos diretamente por (7), considerando que a carga de tráfego é constante para determinada simulação e que um valor arbitrário seja atribuído ao parâmetro μ_c. No modelo de geração de falhas, o tempo inicial para ocorrência de falha é $t_a > 0$, em um ponto que a probabilidade de bloqueio da rede esteja estabilizada. Isso é feito porque no início da simulação há poucas conexões de rede alocadas e muitos recursos disponíveis. Conforme a rede atende as demandas de conexão para determinada carga de tráfego, a probabilidade de bloqueio aumenta e tende a estabilizar em um patamar, como mostrado na Figura 53. Portanto, a curva de probabilidade de bloqueio possui duas regiões, uma em regime transiente e outra em regime permanente de BP. As falhas são inseridas na janela de operação que corresponde ao regime permanente de probabilidade de bloqueio. Isso se deve a dois motivos:

1) Não há sentido em inserir uma falha em uma rede sem ou com poucas conexões ativas;

2) Uniformizar a obtenção das métricas para todas as ocorrências de falha.

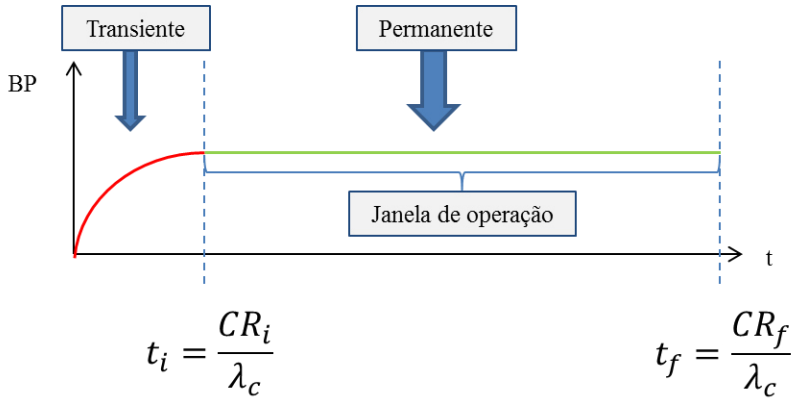


Figura 52 - Janela de operação para inserção de falhas

Considerar a Figura 52. Seja CR a enésima demanda de conexão. Definimos CR_i a demanda de conexão no momento que a probabilidade de bloqueio no começo da região estabilizada e CR_f a última demanda de conexão atendida. Sabe-se que o tempo médio entre chegadas é $\frac{1}{\lambda_c}$. Assim, o tempo no inicio de estabilização da BP é $t_i = \frac{CR_i}{\lambda_c}$ e o tempo final do último atendimento de conexão é $t_f = \frac{CR_f}{\lambda_c}$. A janela de tempo no regime permanente é calculada por (21). Sendo assim, seja N_f o número total de falhas e Δt a janela de ocorrência de falhas, então a taxa média entre as ocorrências de falha λ_f é dado por (22),

$$\Delta t = \frac{(CR_f - CR_i)}{\lambda_c} \quad (21)$$

$$\lambda_f = \frac{N_f}{\Delta t} \quad (22)$$

A disponibilidade da rede descreve a capacidade de seus componentes para operar sem falhas. Há inúmeras medidas de disponibilidade: de nó, de enlace, de conexão. Nesse trabalho, adota-se o conceito de disponibilidade global da rede que é a relação entre o tempo total de funcionamento da rede sem a presença de falhas sobre o tempo total de operação. Assim, seja o tempo médio de falhas (*mean time to failure*, MTTF) $\frac{1}{\lambda_f}$ e o tempo médio que a rede permanece com falhas (*mean downtime*, MDT) $\frac{1}{\mu_f}$. Para um grande número de eventos, a disponibilidade de rede com reparação perfeita é dado por [46],

$$A = \frac{MTTF}{MTTF+MDT} \quad (23)$$

Dado um valor de disponibilidade para uma rede, o parâmetro taxa de restauração de falha μ_f é calculado por,

$$\mu_f = \frac{A\lambda_f}{1-A} \quad (24)$$

Calculados os parâmetros, os tempos dos eventos de ocorrência e restauração de falha podem ser calculados de acordo com o diagrama de fluxo da Figura 53. A variável de tempo é iniciada com $t_a = \frac{CR_i}{\lambda_c}$ e o contador de falhas ID_F $= 0$. Para cada falha calculam-se (17) e (18), depois (19) e, em seguida, (20). Os tempos t_a e t_d obtidos são atribuídos aos eventos de ocorrência de falha e reparação de falha, respectivamente. Após a geração de todos os eventos de falhas, o conjunto de eventos é adicionado aos eventos de conexões e ordenado em ordem crescente utilizando o atributo "tempo" como chave de ordenação.

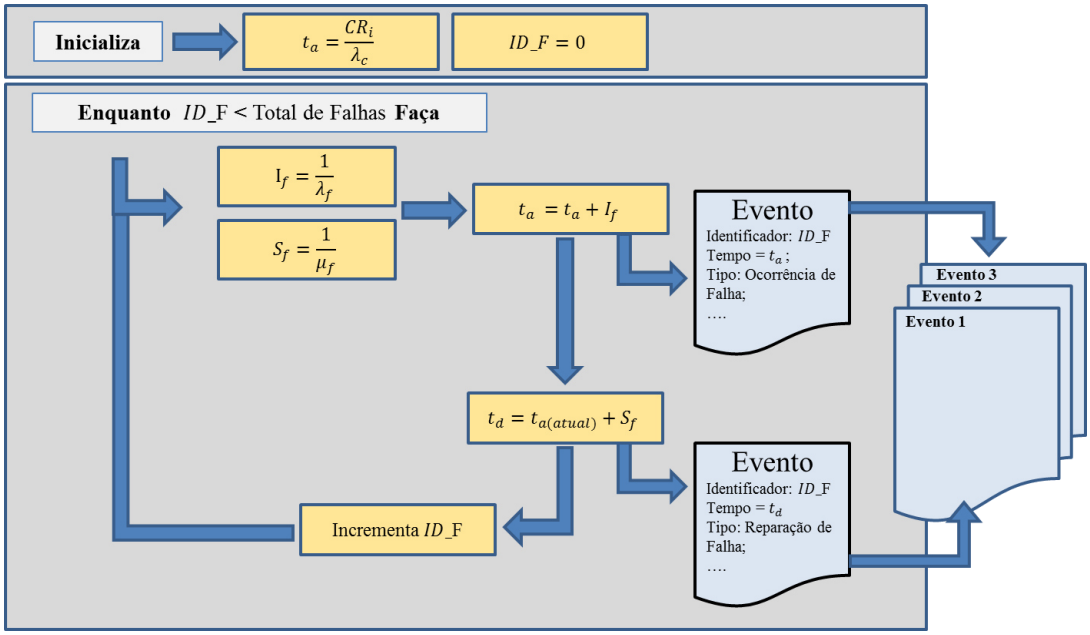


Figura 53 - Diagrama simplificado de geração de eventos de ocorrência e reparação de falha

5.2 Métricas Utilizadas

As métricas adotadas para avaliação de desempenho incluem a probabilidade de bloqueio (*blocking probability*, BP), (25), taxa de utilização do espectro (*spectrum utilization ratio*, SUR), (26), número médio de hops (*average hop*, AHOP), (29), e taxa de restauração de falha (*failure restoration ratio*, FRR), (30). Além das métricas principais, duas métricas auxiliares são utilizadas em algumas comparações: número médio de hops dos caminhos primários e número médio de hops dos caminhos de backup, respectivamente, *Primary* AHOP, (27), e *Backup* AHOP, (28). Estes valores médios estatísticos são obtidos ao final do atendimento de todas as N conexões de entrada definidas para cada intensidade de tráfego. O limite superior teórico para esta métrica nos casos em que o menor caminho é computado sem a utilização de heurísticas é dado pela Tabela 8.

Tabela 8 – Limite superior teórico de AHOP

AHOP Teórico	**NSFNET**	**USNET**
AHOP Primary	2,37	3,05
AHOP Backup	3,62	4,08
AHOP Total	6,00	7,13

A BP, principal medida de desempenho utilizada em redes, é a razão entre o número de conexões bloqueadas pela rede e o número total de conexões geradas. Para computar a BP, primeiramente é preciso um contador que incrementa toda vez que uma conexão de entrada é bloqueada. Como o número total de conexões de entrada é um valor conhecido, basta que ao final da simulação a BP seja calculada por

$$BP = \frac{NumConexões_{Bloquadas}}{NumConexões_{Entrada}} \quad (25)$$

Quanto menor a BP, maior a capacidade de atender novas demandas de conexão.

A métrica SUR é a razão entre o número total de FSUs alocados pelos caminhos secundários (ou caminhos de proteção) e número total de FSUs alocados pelos caminhos primários de cada conexão. Para calcular essa métrica é preciso dois contadores, um para contabilizar a alocação de todos os FSUs ao longo dos caminhos primários, e outro para

contabilizar todos os FSUs alocados ao longo dos caminhos secundários. Ao final da simulação essa razão é calculada por

$$SUR = \frac{NumFSU_{Secundário}}{NumFSU_{Primário}} \quad (26)$$

Quanto menor a SUR melhor a eficiência do espectro, ou seja, significa que os recursos são utilizados mais para atender caminhos de trabalho do que reservados para proteção.

Em seguida, a métrica AHOP é a relação entre o número total de hops dos caminhos primários e secundários das conexões sobre o número total de conexões atendidas. O AHOP é calculado por

$$\text{Primary AHOP} = \frac{NumTotalHOPS_{Primário}}{NumConexões_{Atendidas}} \quad (27)$$

A métrica AHOP pode ser obtida indiretamente pela soma de suas métricas auxiliares *Primary* AHOP e *Backup* AHOP, respectivamente calculadas por

$$\text{Backup AHOP} = \frac{NumTotalHOPS_{Secundário}}{NumConexões_{Atendidas}} \quad (28)$$

$$\text{AHOP} = \frac{NumTotalHOPS_{Primários+Secundário}}{NumConexões_{Atendidas}} \quad (29)$$

O número médio de *hops* das conexões atendidas reflete a quantidade total (valor absoluto) de FSUs alocados ao longo dos caminhos primários e secundários, ou seja, os caminhos com um número maior de hops tendem a alocar mais recursos.

Por último, a métrica FRR é a razão entre o número de conexões restabelecidas (não desconectadas) e o número total de conexões afetadas pelas falhas. Uma razão FRR maior significa uma maior capacidade de sobrevivência da rede. A FRR é calculada por

$$FRR = \frac{NumConexões_{Recuperadas}}{NumConexões_{Afetadas\ por\ falha}} \quad (30)$$

5.3 Formulação do Problema

As topologias de rede adotadas são NSFNET (14 nós, 21 enlaces) e USNET (24 nós, 43 enlaces) como mostram as Figuras 54 e 55, respectivamente. As redes são construídas de acordo com o modelo apresentado na Seção 5.1.1, simbolicamente representadas por um grafo do tipo $G(V, L, F)$, onde $V = \{v_1, v_2, v_3, \dots, v_n\}$ denota o conjunto de vértices que representam os nós da rede, $L = \{l_1, l_2, l_3, \dots, l_m\}$ é o conjunto de arestas que representam os enlaces da rede e $F = \{f_1, f_2, f_3, \dots, f_k\}$ é o conjunto de *FSUs*. Os valores $n, m\ e\ k$, correspondem, respectivamente, ao número máximo de nós, enlaces e *FSUs*.

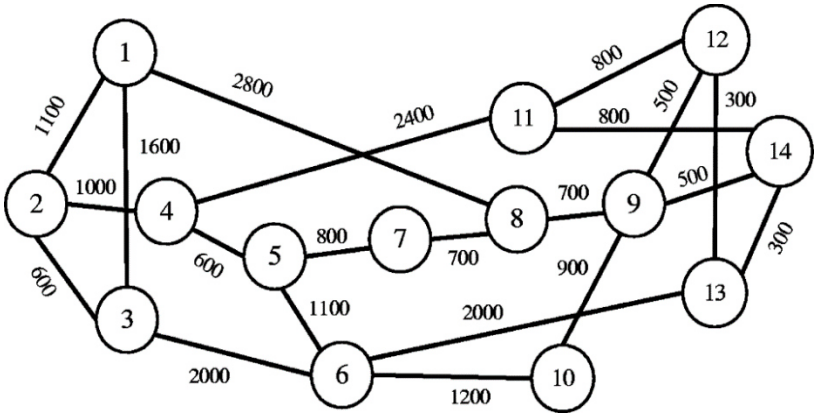


Figura 54: Topologia de rede NSFNET [8]

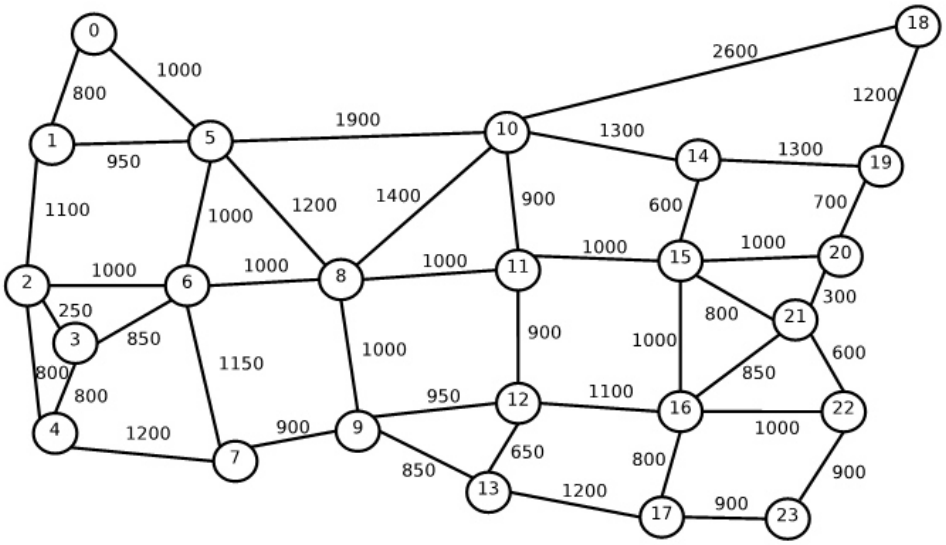


Figura 55: Topologia de rede USNET [8].

Em cada nó da rede EON, supõe-se uma arquitetura com um número de BV-Ts suficientes para atender a demanda de tráfego. O sistema opera na faixa do espectro

eletromagnético correspondente à banda C (Figura 1) e foi escolhida uma banda de 2500 GHz. A largura espectral de cada subportadoras é de 12,5 GHz, sendo este o tamanho de um FSU. O número total de FSUs que constitui a banda é 200. Supõe-se também que cada enlace da rede é composto por um par de fibras, que garante transmissão bidirecional do tráfego e, assim, a sua representação por matriz de adjacência é diagonalmente espelhada e cada *hop* tem custo unitário.

Os eventos de conexões e de falhas seguem o modelo de geração de tráfego e de falhas da Secção 5.1.3. As curvas são obtidas por um conjunto de simulações variando-se a carga de tráfego no intervalo 80 a 400 *erlangs*, com incrementos de 10 *erlangs.* Para cada carga de tráfego, ϱ, são geradas um total de $CR_f = 10^6$ demandas de conexão com taxa de serviço $\mu_c = 1$ e a taxa entre chegadas de conexão é obtida por (7), ou seja, $\lambda_c = \varrho$. A quantidade de banda requerida para cada demanda varia com distribuição uniforme no intervalo [4,8], e as bandas de guardas não são consideradas. Em cada simulação o total de falhas geradas é $N_f = 10^3$ e assume-se que a probabilidade de bloqueio se estabilize a partir da demanda de conexão $CR_i = 5 \times 10^3$. Para cada janela de operação dada por (21), a taxa de ocorrência de falhas λ_f é calculada por (22) e dado que a disponibilidade de rede é $A = 0{,}99$, a taxa de manutenção de falhas μ_f é calculada por (24).

Os algoritmos RSA testados são tratados separadamente em subproblemas (Seção 4). Primeiro resolve-se o subproblema de roteamento representando a topologia de rede com uma matriz de adjacência e utilizando o algoritmo de *Dijkstra* conforme explicado na Seção 4.1. Em seguida, resolve-se o subproblema de alocação de espectro utilizando o algoritmo *first-fit* segundo a Seção 4.2. Ao algoritmo RSA base *Dijkstra+first-fit* ainda podem ser adicionadas heurísticas como o DLBSPP e IDS. Além disso, podem ser implementados os esquemas de proteção e restauração DPP, SPP, TAR e BSR, como descritos na Seção 3. Os parâmetros definidos para a heurística DLB são $\alpha = 200$ e $\beta = 2$ e estes foram obtidos por meio de uma calibragem prévia.

Com o intuito de promover melhor entendimento na análise das heurísticas e dos esquemas de proteção e restauração foram definidos cinco grupos de comparação. O **Grupo 1** (Tabela 9) compara o algoritmo RSA implementando esquemas de proteção DPP e SPP com e sem restauração dinâmica. Assim, podem-se comparar diretamente dois esquemas de proteção e também visualizar os efeitos da restauração dinâmica para cada tipo de proteção. O experimento do **Grupo 1** é reproduzido duas vezes, a primeira com ocorrências de uma única

falha e a segunda com ocorrências de 3 falhas simultâneas. Os demais grupos de comparação são tratados com 3 falhas simultâneas.

Tabela 9 - Grupo 1: Comparação entre SPP e DPP, com e sem restauração dinâmica

Grupo 1	Algoritmo RSA	Heurísticas	Proteção	Restauração
SPP vs DPP	Dijkstra+FF	Nenhuma	SPP	Nenhuma
	Dijkstra+FF	Nenhuma	DPP	Nenhuma
	Dijkstra+FF	Nenhuma	SPP	Restauração dinâmica
	Dijkstra+FF	Nenhuma	DPP	Restauração dinâmica

Utilizando os mesmos esquemas de proteção, realiza-se no **Grupo 2** a comparação entre a restauração dinâmica padrão (*dynamic restoration*, DR) e a restauração do tipo TAR como mostra a Tabela 10.

Tabela 10 - Grupo 2: Comparação entre Restauração dinâmica e restauração TAR

Grupo 2	Algoritmo RSA	Heurísticas	Proteção	Restauração
Restauração dinâmica vs TAR	Dijkstra+FF	Nenhuma	SPP	Restauração dinâmica
	Dijkstra+FF	Nenhuma	SPP	TAR
	Dijkstra+FF	Nenhuma	DPP	Restauração dinâmica
	Dijkstra+FF	Nenhuma	DPP	TAR

No **Grupo 3,** é considerado os níveis de serviço de cada conexão e atribuí-se proporções diferentes entre as demandas de conexões, sendo que cada nível de serviço implementa um modelo de recuperação diferente que são: FBGR, PBGR, BER**.** Qualquer configuração que implementa um dos modelos de recuperação citados é chamada restauração BSR. O BSR é comparado também com o a restauração dinâmica padrão (DR), principalmente para que seja extraída uma comparação direta com a restauração BSR com 100% do modelo BER, como mostrado na Tabela 11.

Tabela 11 - Grupo 3: Restauração BSR em diferentes proporções de níveis de serviço.

Grupo 3	Algoritmo RSA	Heurísticas	Proteção	Restauração (FBGR, PBGR, BER)
BRS diferentes níveis de serviço	Dijkstra+FF	Nenhuma	DPP	BSR (100-0-0)
	Dijkstra+FF	Nenhuma	DPP 50%	BSR (0-100-0)
	Dijkstra+FF	Nenhuma	Nenhuma	BSR (0-0-100)
	Dijkstra+FF	Nenhuma	Misto	BSR (33,33,34)
	Dijkstra+FF	Nenhuma	Nenhuma	DR

O **Grupo 4** (Tabela 12) e **Grupo 5** (Tabela 13) são grupos de comparação correlacionados, que tratam do esquema de proteção SPP e suas combinações heurísticas: SPP, DLBSPP, SPP+IDS, DLBSPP+IDS. No **Grupo 4**, o reestabelecimento das conexões no caso de falha é feito apenas pela comutação dos caminhos de proteção. No **Grupo 5**, as conexões que não puderam ser reestabelecidas pela comutação dos caminhos de proteção são restauradas dinamicamente utilizando os recursos disponíveis na rede no momento da falha.

Tabela 12 - Grupo 4: Comparação SPP, DLBSPP, SPP+IDS, DLBSPP+IDS sem restauração

Grupo 4	Algoritmo RSA	Heurísticas	Proteção	Restauração
SPP e heurísticas s/restauração	Dijkstra+FF	Nenhuma	SPP	Nenhuma
	Dijkstra+FF	DLB	SPP	Nenhuma
	Dijkstra+FF	IDS	SPP	Nenhuma
	Dijkstra+FF	DLB+IDS	SPP	Nenhuma

Tabela 13 - Grupo 5: Comparação SPP, DLBSPP, SPP+IDS, DLBSPP+IDS com restauração

Grupo 5	Algoritmo RSA	Heurísticas	Proteção	Restauração
SPP e heurísticas c/restauração	Dijkstra+FF	Nenhuma	SPP	Restauração dinâmica
	Dijkstra+FF	DLB	SPP	Restauração dinâmica
	Dijkstra+FF	IDS	SPP	Restauração dinâmica
	Dijkstra+FF	DLB+IDS	SPP	Restauração dinâmica

6 ANÁLISE DOS RESULTADOS

Os grupos de comparação apresentados na Seção 5.3 correspondem ao conjunto de simulações em varredura de carga de tráfego. Cada simulação utiliza as heurísticas e os esquemas de proteção e restauração listados nas tabelas 9 a 13. O conjunto de métricas, descrito na Seção 5.2, é obtido para cada simulação e os resultados apresentados em gráficos e complementados por tabelas. Os gráficos gerados são: BP, SUR, AHOP, Primary AHOP, Backup AHOP e FRR. Para cada gráfico, são mostrados os resultados das simulações realizadas nas topologias NSFNET e USNET, nesta ordem. Os gráficos possuem duas regiões distintas de carga de tráfego, como mostrado na Figura 56. A região mais à esquerda corresponde a de carga baixa (CB) de tráfego e a região mais a direita corresponde à carga alta (CA). Na região CB, a rede dispõe de muitos recursos, por isso a probabilidade de bloqueio é baixa. Na região CA, os recursos da rede se tornam escassos e a probabilidade de bloqueio aumenta.

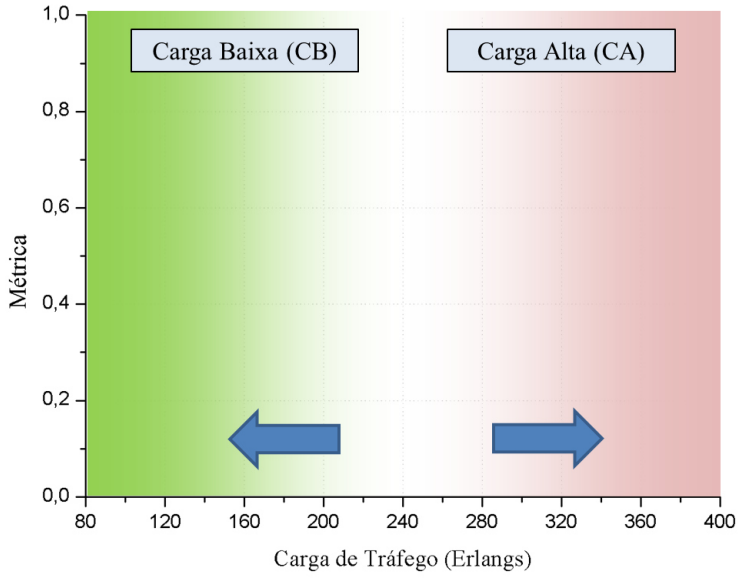


Figura 56 - Regiões de carga baixa e carga alta de tráfego.

Dado essa forma de apresentar os resultados, a análise é realizada de acordo com as seguintes premissas:

Premissa 1) A probabilidade de que ocorra uma alocação de espectro em um enlace é inversamente proporcional ao seu estado de ocupação, ou seja, quanto menos carregado o enlace, maiores as chances de alocação e vice versa;

Premissa 2) Um caminho secundário contém no mínimo o mesmo número de hops do seu respectivo caminho primário;

Premissa 3) O número total de recursos alocados para um caminho dedicado é a quantidade de banda requerida vezes o número de hops do caminho;

Premissa 4) O número total de recursos alocados para um caminho compartilhado é a quantidade de banda requerida vezes o número de hops do caminho menos o número de slots compartilhados;

Premissa 5) Quanto maior a granularidade da banda requerida, menor a probabilidade de uma alocação que satisfaça as restrições de continuidade e consecutividade;

Premissa 6) Quanto maior o número de hops de um caminho, menor a probabilidade de uma alocação que satisfaça das restrições de continuidade e consecutividade.

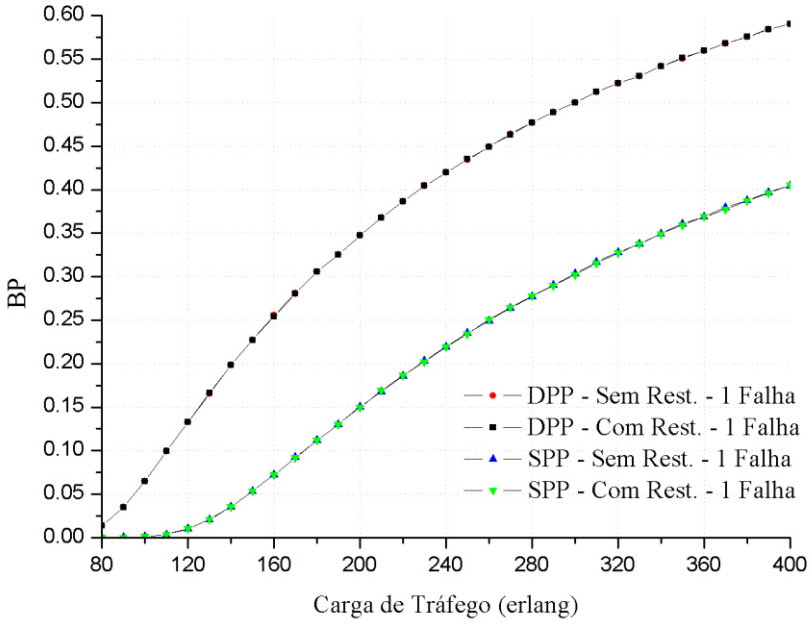
6.1 Resultados do Grupo 1 – SPP x DPP

As simulações desse grupo de comparação são realizadas para uma única falha e para três falhas simultâneas. Nesse experimento, a análise das simulações será realizada de acordo com as seguintes métricas: BP, SUR, AHOP, *Primary* AHOP, *Backup* AHOP, FRR.

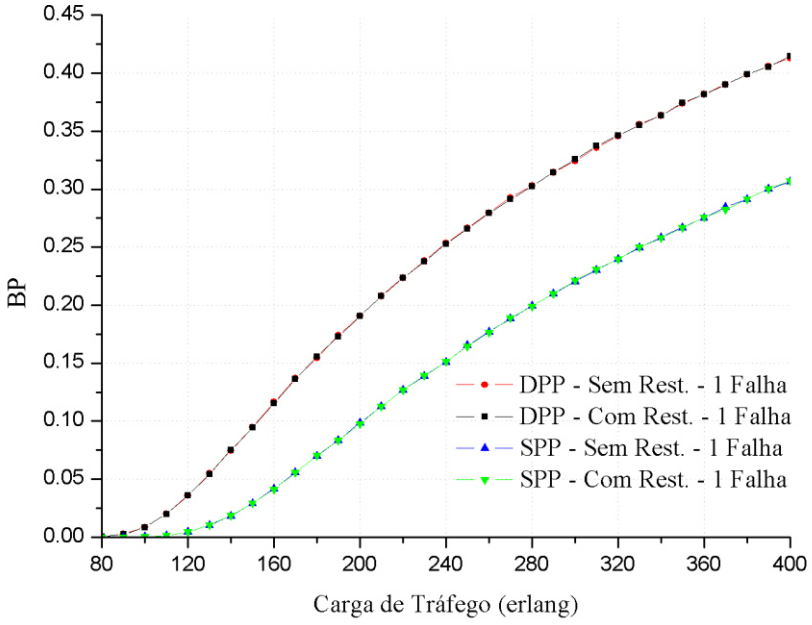
6.1.1 Para uma única falha

O gráfico de BP é apresentado na Figura 57. As curvas com e sem restauração de cada esquema estão sobrepostas, portanto, a análise será feita observando a relação entre os esquemas SPP e DPP, ignorando por enquanto a aplicação da restauração dinâmica em cada uma delas. Em ambas as topologias, a BP das curvas tendem a aumentar da região de CB para região de CA. Isso ocorre porque com o aumento da carga de tráfego, aumenta-se a o nível de ocupação da rede e, segundo a **premissa 1**, essa escassez de recursos na região de CA é responsável pelo aumento da BP. Considerando essa relação de “ocupação da rede” e “probabilidade de bloqueio”, pode-se justificar o fato de que, em ambas as regiões de carga e

topologias, o esquema SPP exibe menor BP do que o DPP, pois o esquema DPP consome mais recursos de rede para alocar seus caminhos de *backup*. Em topologias menores, como a NSFNET, os recursos se esgotam mais rapidamente, por isso o aumento da BP é mais acentuado.



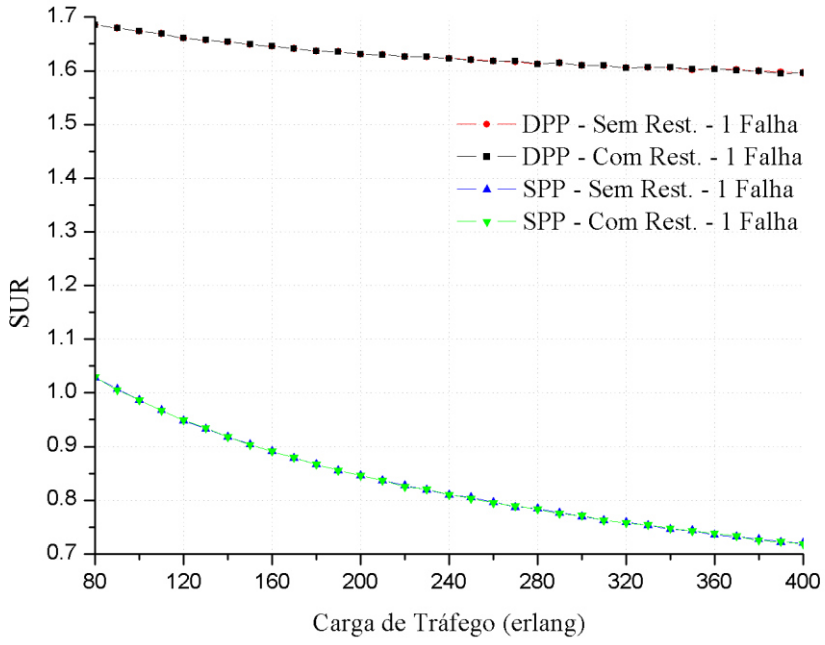
a)



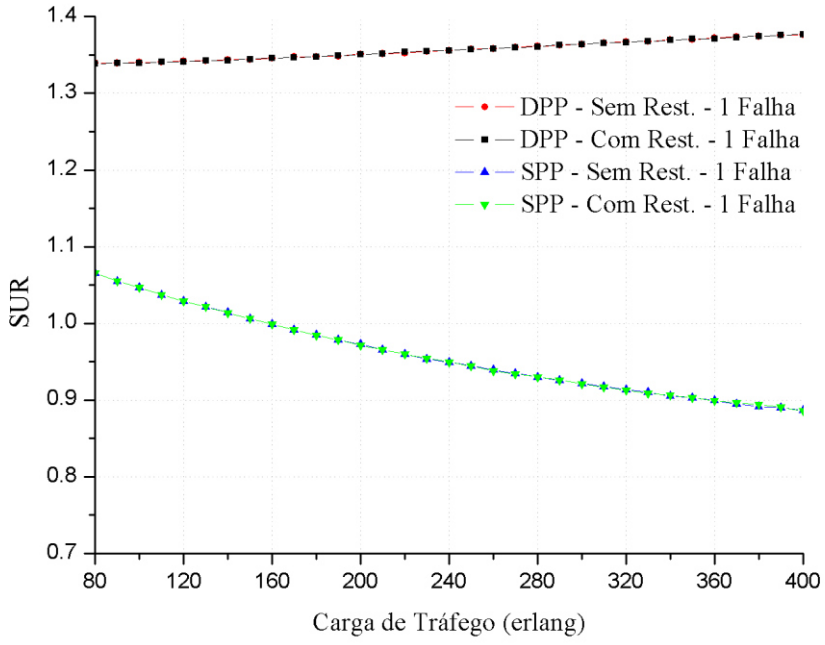
b)

Figura 57 - Gráfico de BP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET.

A baixa BP obtida pelo SPP em relação ao DPP se deve à sua característica de compartilhamento de recursos nos caminhos de proteção. Quanto mais os recursos são compartilhados, mais recursos ficam disponíveis para atender novas demandas de conexão. A relação entre a quantidade de recursos alocados que atendem os caminhos secundários e os caminhos primários é dada pela SUR na Figura 58. A Tabela 14 mostra essas quantidades em números absolutos. Observa-se que, com a carga de tráfego em 80 erlangs, em que a BP é próxima de zero, o número de recursos alocados pelos caminhos primários para ambos os esquemas é praticamente igual, porém, o número de recursos alocados pelos caminhos secundários é menor para o esquema SPP (**premissa 4**) e, consequentemente, a sua SUR é menor. Quando se aumenta a carga de tráfego para 240 e 400 *erlangs*, a quantidade total de recursos alocados para os caminhos primários e secundários diminui. Essa diminuição do total de recursos é esperada, uma vez que a probabilidade de bloqueio aumenta e menos conexões são aceitas. Ao analisar os valores absolutos entre os esquemas DPP e SPP, mostra que os recursos que o esquema SPP permite economizar por meio do compartilhamento são utilizados no atendimento de novas demandas de conexão e, consequentemente, resulta no aumento do número total de recursos alocados pelos caminhos primários. Dessa forma, o esquema SPP diminui o número total de recursos que atendem os caminhos secundários, por meio do compartilhamento de slots, e aumenta o número total de recursos que atendem os caminhos primários. Esses dois efeitos combinados contribuem para que a curva SUR do esquema SPP apresente um declínio na região de CA.



a)



b)

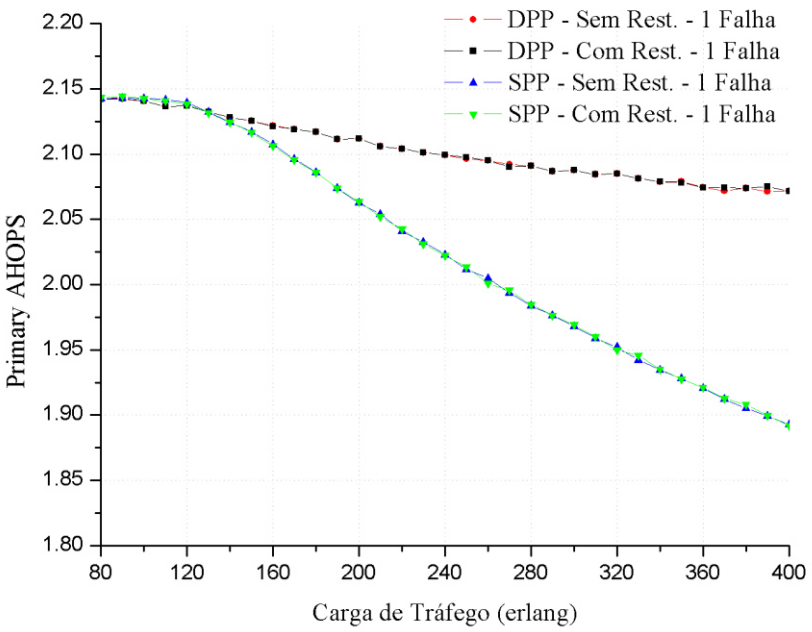
Figura 58 - Gráfico de SUR comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET.

Tabela 14 - Quantidade total de recursos alocados para os esquemas DPP e SPP sem restauração(x 1 milhão).

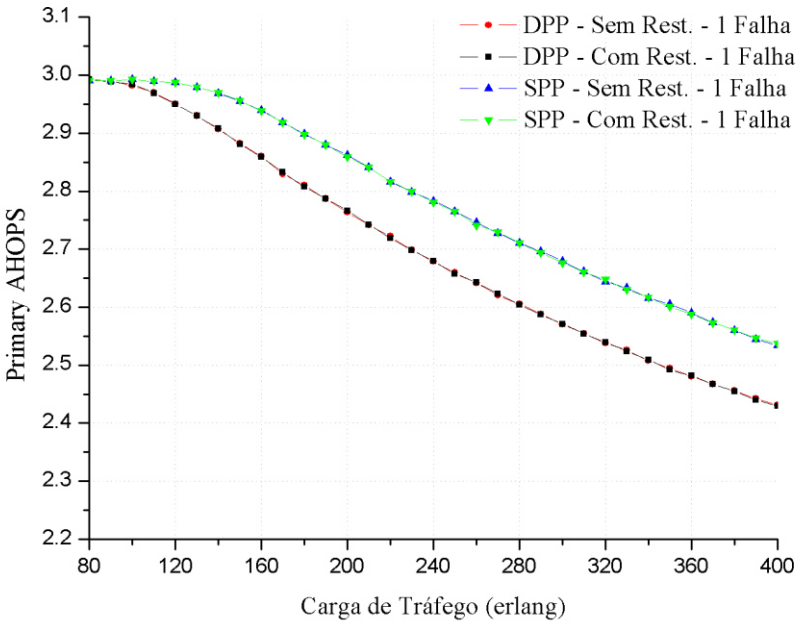
Curvas	Topologia	80 erlangs		240 erlangs		400 erlangs	
		Primário	Secundário	Primário	Secundário	Primário	Secundário
DPP	NSFNET	12,645	21,312	6,692	10,862	4,461	7,121
SPP		12,853	13,224	9,018	7,308	6,184	4,455
DPP	USNET	17,945	24,034	11,366	15,409	7,8934	10,863
SPP		17,944	19,119	13,688	12,997	9,906	8,781

No esquema SPP, a magnitude da SUR depende do número de compartilhamentos efetuados. Quanto mais recursos são compartilhados, menor a SUR. No esquema DPP a SUR mínima é 1, que pode ser deduzido considerando que os caminhos primários e secundários possuam o mesmo comprimento mínimo (**premissa 2**) e, assim, a quantidade total de recursos alocados ao longo das rotas é a mesma. Na prática, esse valor é maior do que 1.

Os gráficos de *Primary* AHOP (Figura 59) e *Backup* AHOP (Figuras 60) mostram o número médio de hops dos caminhos primários e o número médio de hops dos caminhos secundários. Segundo esses gráficos, observa-se que o *Backup* AHOP é maior do que o *Primary* AHOP em toda varredura de carga para ambas as topologias. Por isso, a quantidade média de recursos alocados para os caminhos de *backup* é maior do que a quantidade média de recursos alocados para os caminhos primários. Essa diferença do AHOP entre os caminhos primários e secundários reflete diretamente na magnitude da SUR do esquema DPP.

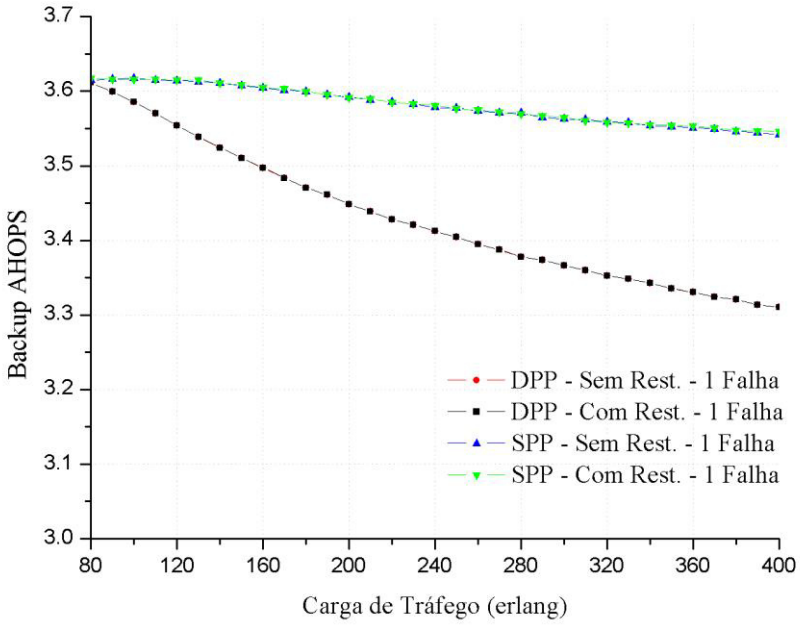


a)

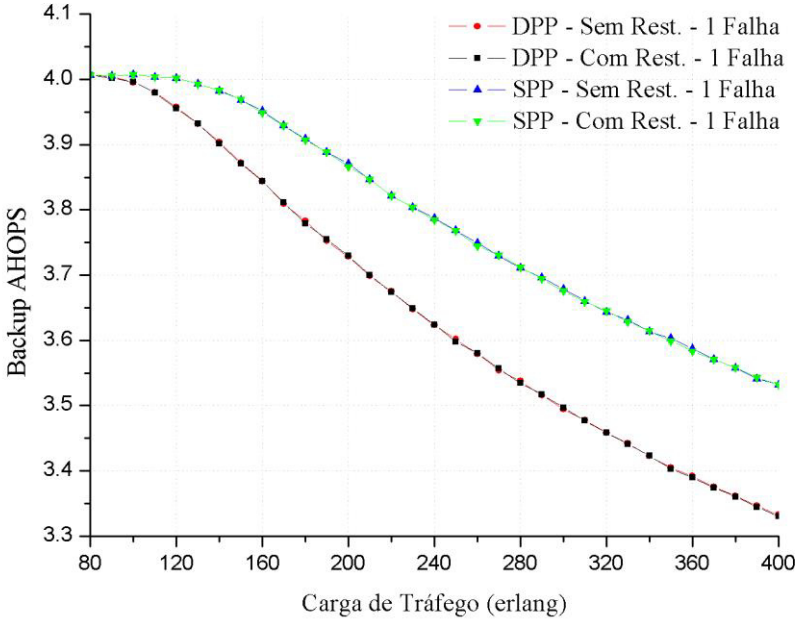


b)

Figura 59 - Gráfico de *Primary* AHOP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET.



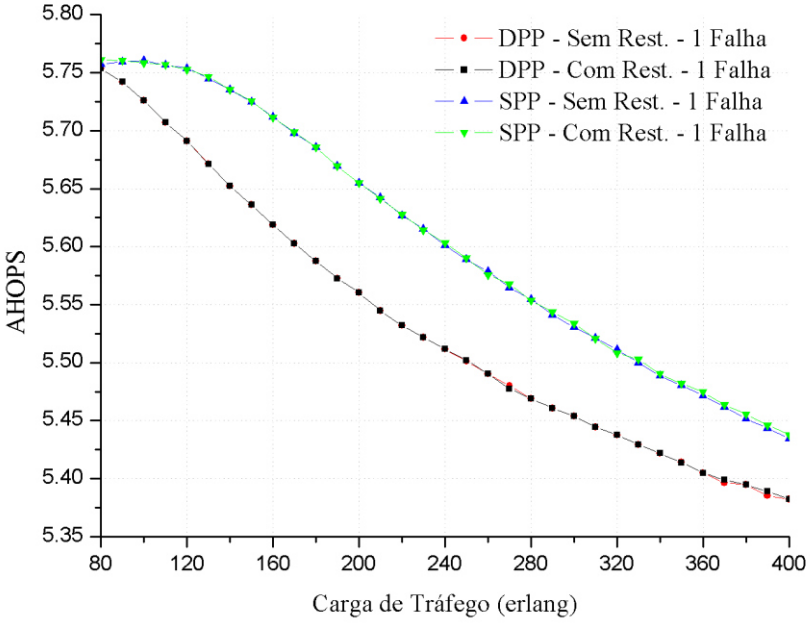
a)



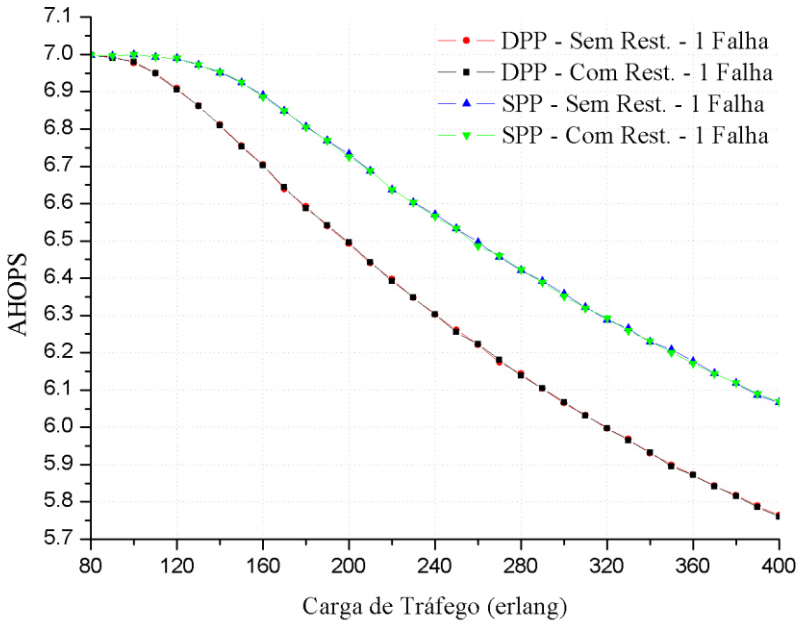
b)

Figura 60 - Gráfico de *Backup* AHOP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET.

A métrica seguinte, AHOP (Figura 61), apresenta uma diminuição conforme se aumenta a carga de tráfego. A diminuição do número médio de hops na região de CA se deve ao aumento da BP, cujas conexões contenham caminhos com maiores números de hops. Tendo em vista a **premissa 6**, conclui-se que o menor número de recursos disponíveis na região de CA tende a diminuir a probabilidade em atender as restrições de continuidade e consecutividade na alocação e, assim, as conexões cujos caminhos têm um maior número de hops são mais penalizadas, aumentando-se as chances de serem bloqueadas. Conexões bloqueadas não são contabilizadas no AHOP e, portanto, quanto mais bloqueio de conexões com caminhos mais longos, menor é o AHOP. Por isso, as curvas do esquema SPP apresentam um AHOP maior, por tem menor BP, permite alocar conexões com caminhos mais longos (devido a maior quantidade de recursos livres promovidos pelo compartilhamento).



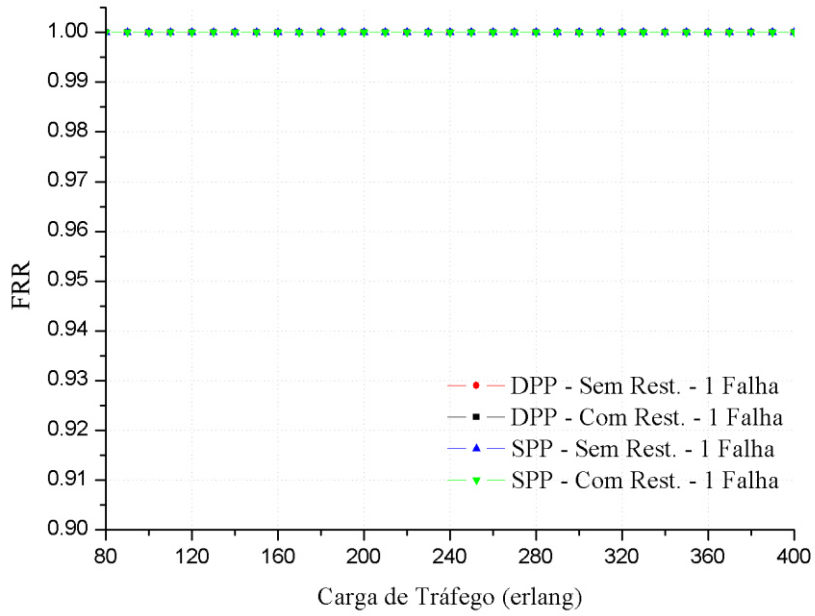
a)



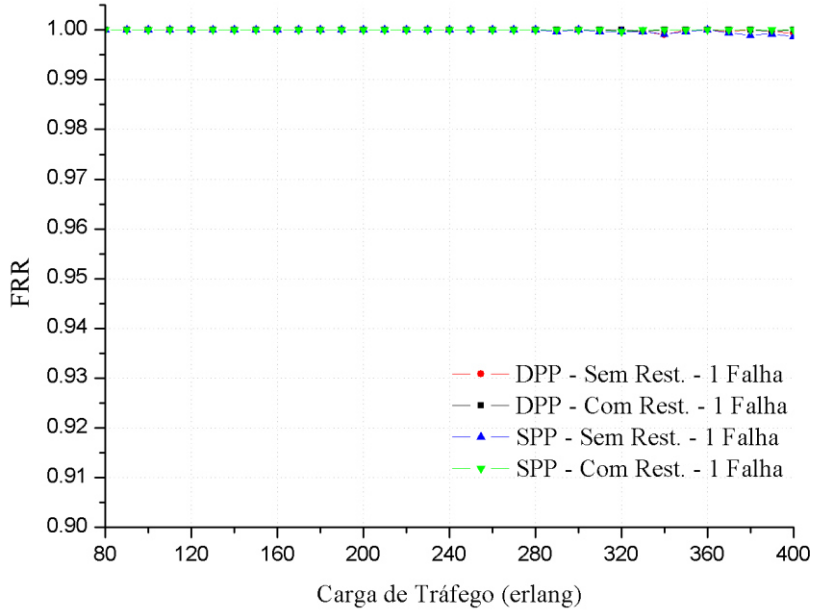
b)

Figura 61 - Gráfico de AHOP comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET.

Por último, as curvas de FRR (Figura 62) em todos os casos apresentam valores que tendem à ‘1’, em toda varredura de carga. Este resultado é coerente com as expectativas teóricas: 1) em um DPP um caminho de proteção dedicado é reservado e, no caso de uma única falha, a proteção é garantida e; 2) em um SPP, o caminho de proteção dá suporte para caminhos primários disjuntos, sendo que na ocorrência de uma única falha, dois caminhos primários não concorrem pela obtenção da proteção. Para que esse resultado de fato ocorra, o espaçamento entre os tempos de ocorrência de falha devem ser maiores do que o tempo de manutenção da conexão. Dessa forma, duas falhas consecutivas não ocorrem em uma mesma conexão. Nessas circunstâncias, a restauração por meio da comutação dos caminhos de proteção provê máxima FRR. Portanto, a restauração dinâmica nesse caso não é relevante. É por isso que praticamente não há diferenças entre as curvas com e sem restauração dinâmica para cada esquema nas métricas analisadas.



a)



b)

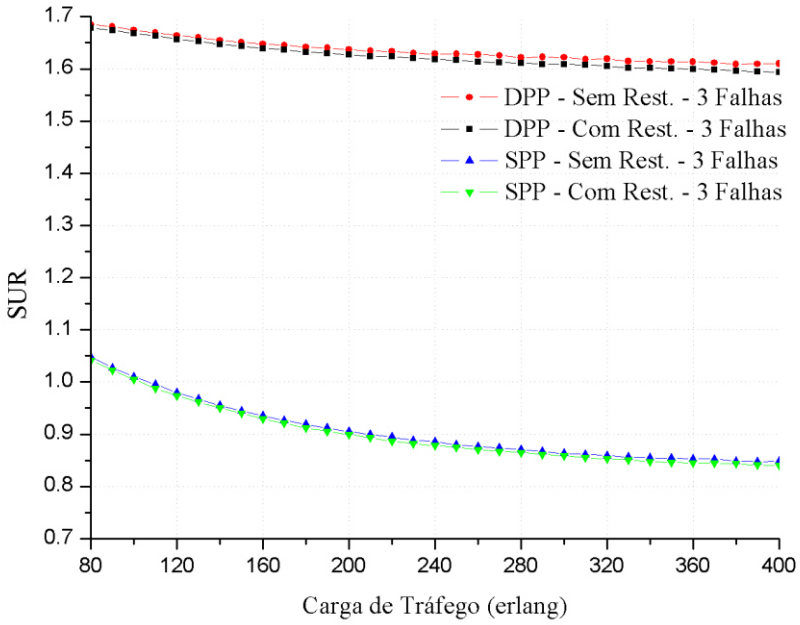
Figura 62 - Gráfico de FRR comparando DPP x SPP com e sem restauração para uma única falha: a) NSFNET; b) USNET.

6.1.2 Para três falhas simultâneas

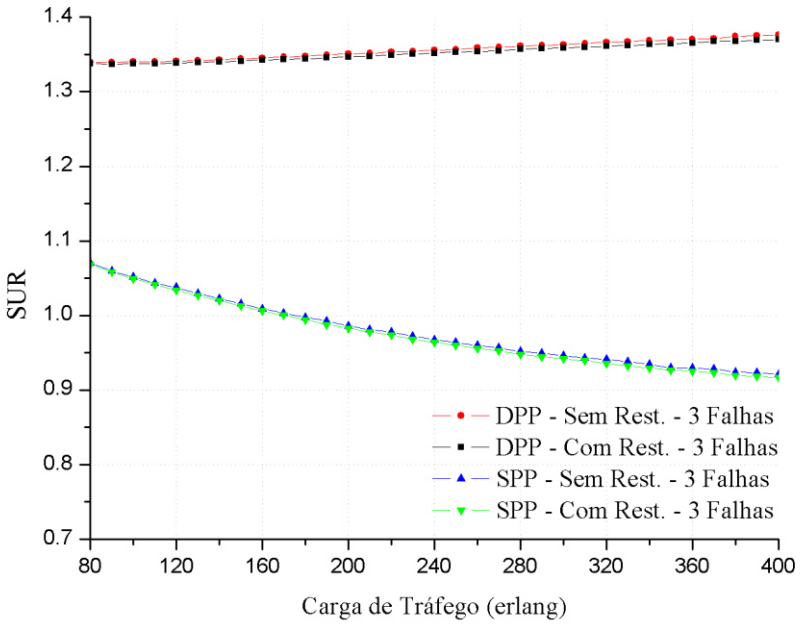
Esse experimento compõe o mesmo grupo de comparação do experimento anterior e a diferença é que neste são inseridas três falhas simultâneas por evento de ocorrência de falha ao invés de apenas uma única falha. No experimento anterior, o uso da restauração dinâmica se mostrou desnecessária, pois foi provado que os esquemas de proteção conseguem recuperar 100% das conexões afetadas no caso de uma única falha. No entanto, neste experimento, devido à ocorrência de múltiplas falhas simultâneas, há possibilidade de que os caminhos primários e secundários sejam afetados ao mesmo tempo e necessite da restauração dinâmica para auxiliar no restabelecimento das conexões.

As considerações feitas sobre as características dos esquemas SPP e DPP são válidas para esse experimento e justifica a maioria das métricas obtidas. Neste sentido, o resultado apresentado no gráfico BP deste experimento é semelhante ao experimento anterior, por isso ele é apresentado no Apêndice F, identificado pela Figura 80. No entanto, pode-se considerar que haja alguma influência no uso da restauração dinâmica nessa métrica, embora seja imperceptível na magnitude em que ela ocorra.

A métrica seguinte é a SUR, apresentada na Figura 63. Nessa métrica, ocorre um efeito de descolamento das curvas que utilizam restauração dinâmica. Nesse caso, a mudança de amplitude nas curvas é mínima, mas perceptível. Toda vez que a restauração dinâmica é executada, um novo caminho primário pode ser alocado e, segundo a **premissa 3**, o número total de recursos que atende os caminhos primários aumenta e consequentemente, a SUR diminui. Como o aumento do número de recursos alocados para os caminhos primários ocorre em pequena proporção, a diminuição da SUR também é pequena para todos os casos. O número total de recursos alocados para os caminhos primários e secundários são tabelados em seguida. A Tabela 15 mostra os valores referentes às curvas obtidas sem restauração dinâmica e a Tabela 16 mostra as curvas com restauração dinâmica. Observa-se que, nas três cargas de tráfego apresentadas, o número de recursos alocados para os caminhos primários na Tabela 16 são maiores do que na Tabela 15.



a)



b)

Figura 63 - Gráfico de SUR comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET.

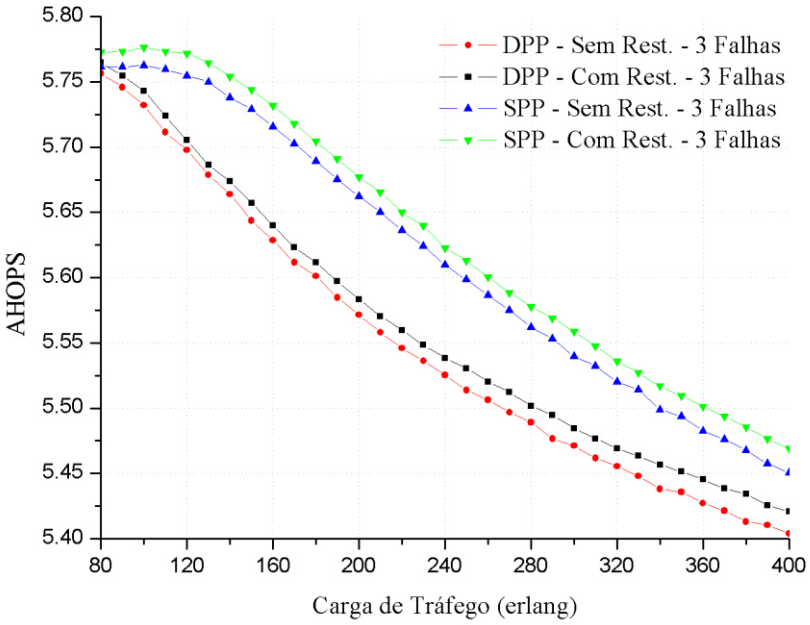
Tabela 15 - Quantidade total de recursos alocados para os esquemas DPP e SPP sem restauração (x 1 milhão).

Curvas	Topologia	80 erlangs		240 erlangs		400 erlangs	
		Primário	Secundário	Primário	Secundário	Primário	Secundário
DPP	NSFNET	12,674	21,353	6,905	11,247	4,684	7,540
SPP		12,859	13,472	9,104	8,065	6,273	5,320
DPP	USNET	17,942	24,035	11,546	15,652	8,100	11,147
SPP		17,951	19,216	13,769	13,321	10,045	9,251

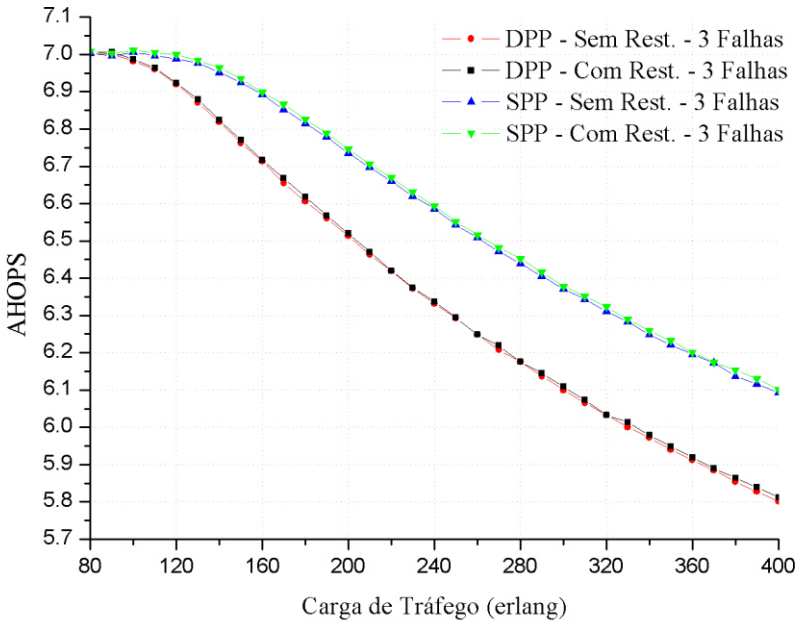
Tabela 16 - Quantidade total de recursos alocados para os esquemas DPP e SPP com restauração (x 1 milhão).

Curvas	Topologia	80 erlangs		240 erlangs		400 erlangs	
		Primário	Secundário	Primário	Secundário	Primário	Secundário
DPP	NSFNET	12,721	21,348	6,928	11,212	4,722	7,528
SPP		12,925	13,462	9,165	8,048	6,312	5,303
DPP	USNET	17,968	24,035	11,574	15,644	8,115	11,117
SPP		17,986	19,213	13,816	13,318	10,06	9,222

Na métrica AHOP (Figura 64), a diferença entre as curvas com e sem restauração dinâmica em cada esquema se deve ao restabelecimento dos caminhos de trabalho que aumenta o número médio de hops para cada conexão. Essa diferença é observada na métrica *Primary* AHOP na Figura 65, mas não na métrica *Backup* AHOP na Figura 66.

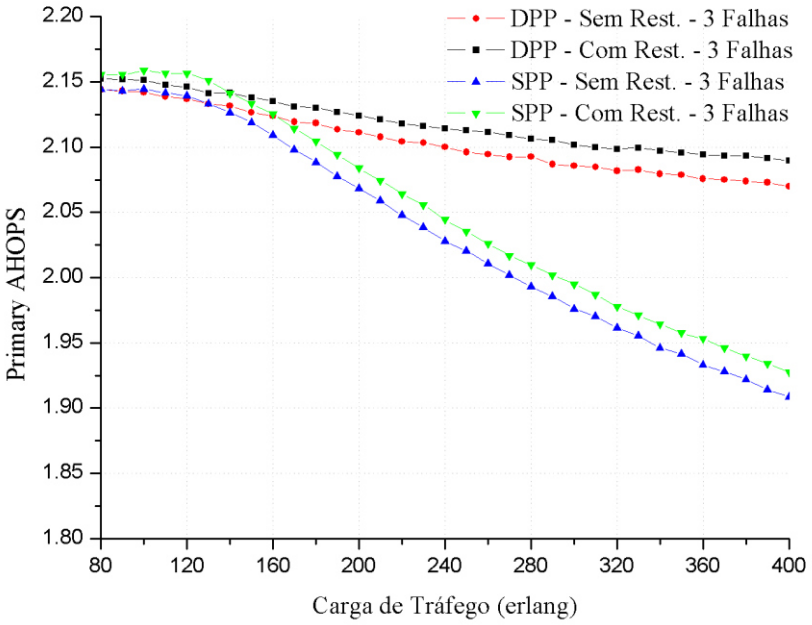


a)

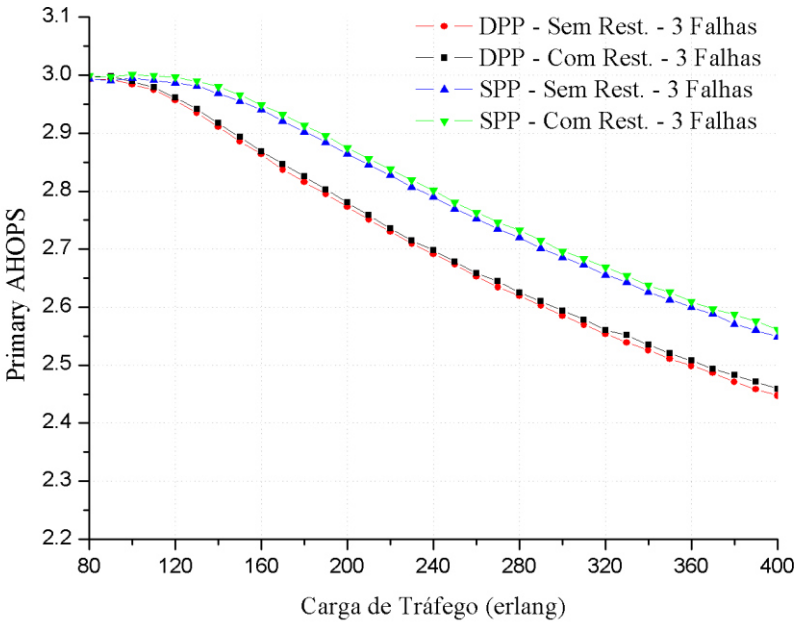


b)

Figura 64 - Gráfico de AHOP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET.

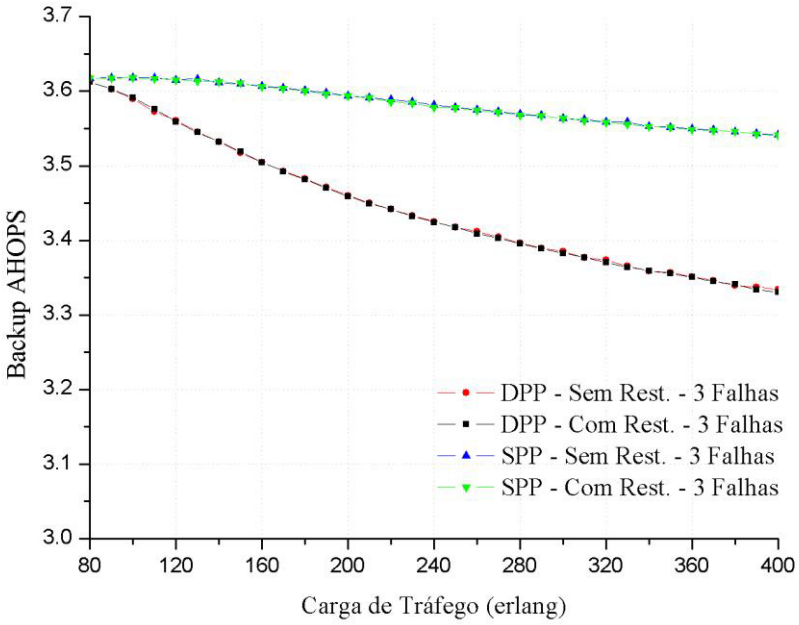


a)

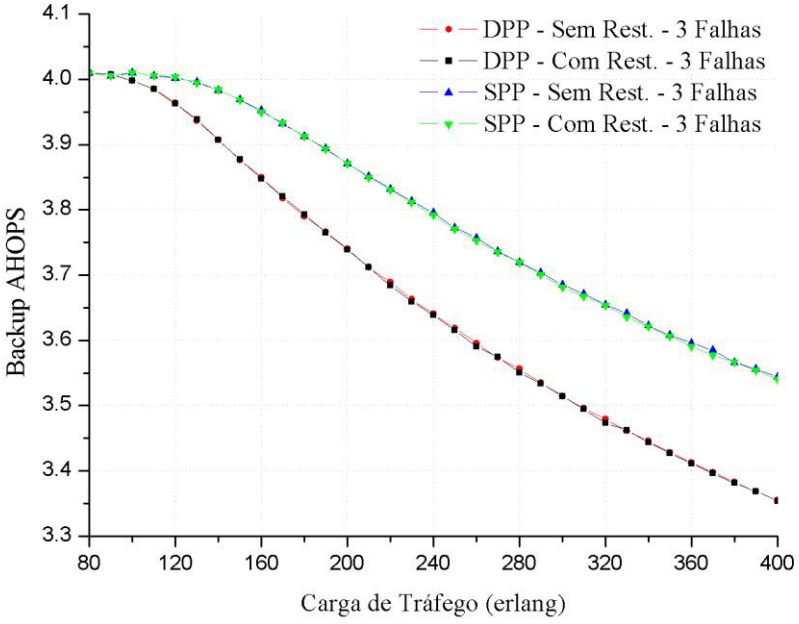


b)

Figura 65 - Gráfico de *Primary* AHOP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET.



a)

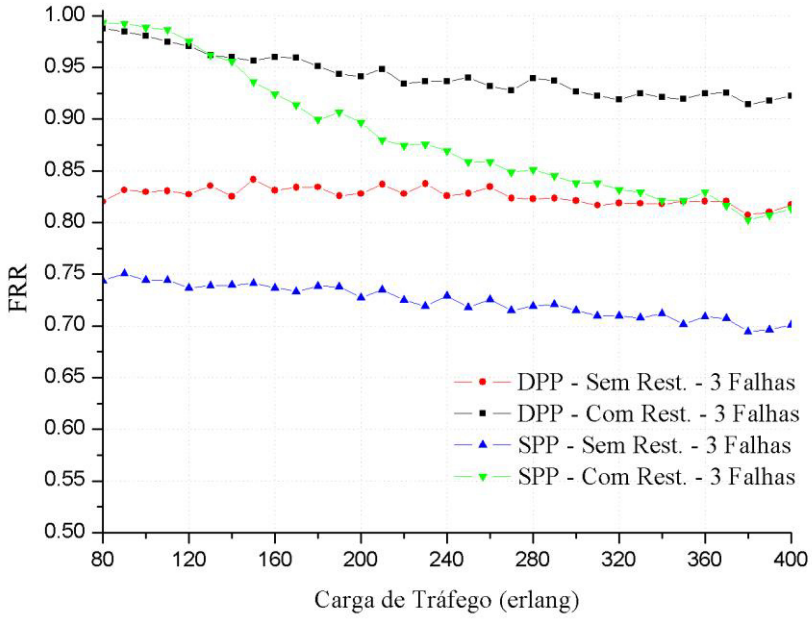


b)

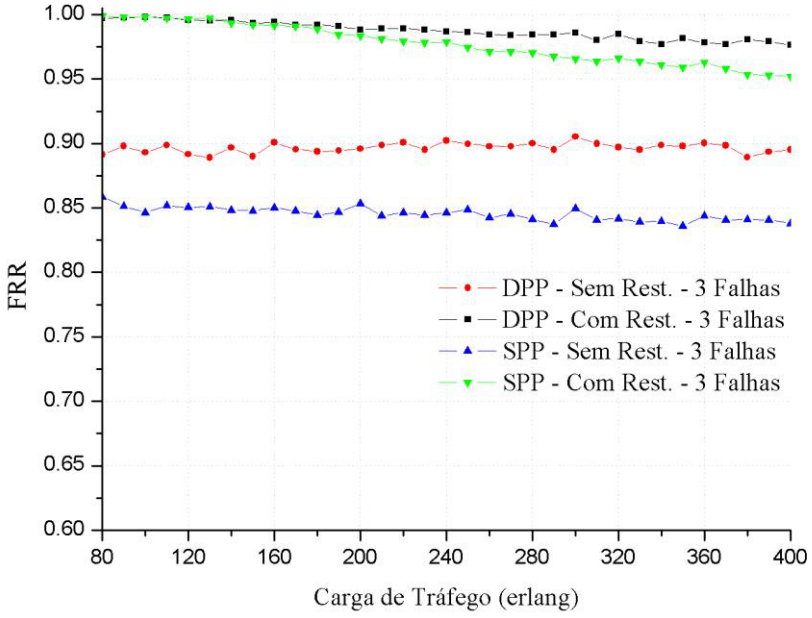
Figura 66 - Gráfico de Backup AHOP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET.

Por último, a métrica FRR é mostrada na Figura 67. Primeiramente, comparam-se as curvas SPP e DPP sem restauração dinâmica. Observa-se que a curva do SPP sem restauração é menor do que o DPP sem restauração em toda varredura de carga de tráfego para as duas topologias. Esse resultado é assim explicado: dado que ocorra uma falha em um enlace que passa um caminho secundário, a probabilidade de que ocorra uma falha em outro enlace que passe pelo seu respectivo caminho primário é maior para o esquema SPP do que para o DPP. No esquema DPP, os recursos de backup que estão alocados no enlace da primeira falha dão suporte a apenas um caminho primário, e no esquema SPP, os recursos compartilhados dão suporte a N caminhos primários. Portanto, as chances de que a segunda falha afete um caminho primário cujo caminho secundário já foi afetado por uma falha é maior para o esquema SPP. Sendo assim, pode-se concluir que o risco de comprometimento das conexões que utilizam esquema SPP é maior do que o DPP devido ao compartilhamento de recursos e, quanto maior o número de compartilhamento, menor a capacidade de restauração por comutação de caminhos.

Na segunda parte dessa análise, é considerado o uso da restauração dinâmica, que resulta em um aumento do FRR em cada caso. O ganho relativo, calculado por (31), da FRR para cada curva sem e com restauração dinâmica é mostrado na Tabela 17. Em todos os casos, o ganho relativo percentual promovido pela restauração dinâmica é maior no SPP do que o do DPP. Um maior ganho de FRR do SPP em relação ao DPP está diretamente relacionado com a capacidade de compartilhamento de recursos que permite economizar recursos e obter uma menor BP.



a)



b)

Figura 67 - Gráfico de FRR comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET.

$$Percentual\ Relativo = \frac{V_{posterior} - V_{anterior}}{V_{anterior}} 100 \qquad (31)$$

Tabela 17 - Ganho relativo percentual de FRR entre os esquemas sem restauração e com restauração

Esquema	Topologia	80 erlangs	240 erlangs	400 erlangs
DPP	NSFNET	20,41%	13,37 %	12,92 %
SPP		33,54%	19,23%	16.04%
DPP	USNET	11,84%	9,36%	9,09%
SPP		16,32%	15,63%	13,65%

6.2 Resultados do Grupo 2 – Restauração Padrão x TAR

Nesse experimento, os esquemas SPP e DPP são combinados com dois tipos de restauração dinâmica. O primeiro é o tipo padrão, que é a restauração dinâmica (*dynamic restoration*, DR) realizada no experimento da Seção 6.1.2 e o segundo é o tipo TAR, explicado na Seção 3.4. As métricas utilizadas nesse experimento são: BP, SUR, AHOP, FRR.

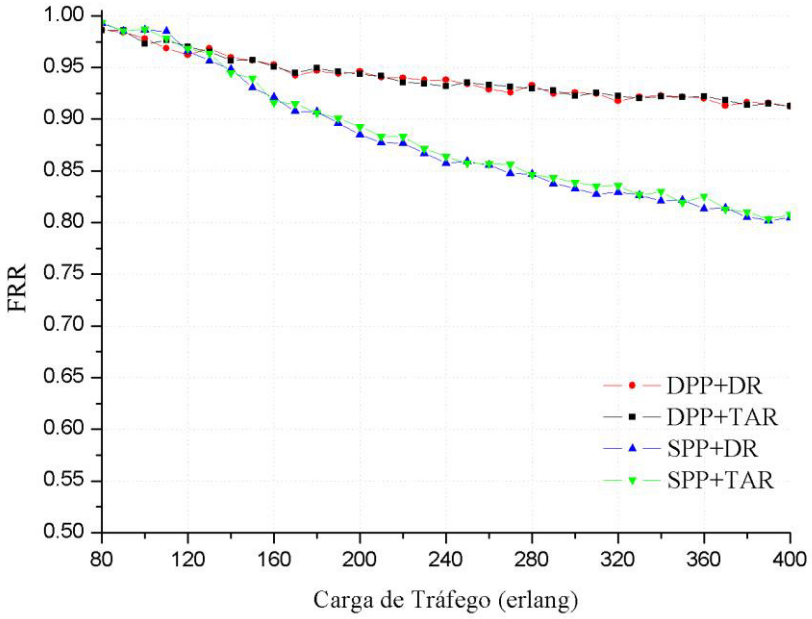
Para compreender a diferença entre as restaurações DR e TAR, é preciso analisar os efeitos causados nas métricas quando se utiliza uma restauração dinâmica qualquer. Uma restauração dinâmica pode alocar novos caminhos de trabalho na tentativa de restabelecer as conexões afetadas por falha, e isso resulta em:

1) Aumento da AHOP, pois um terceiro caminho é alocado para uma conexão;
2) Diminuição da SUR, porque um maior número de recursos é alocado para os caminhos de trabalho;
3) Aumento da BP, com mais recursos alocados e maior ocupação da rede.

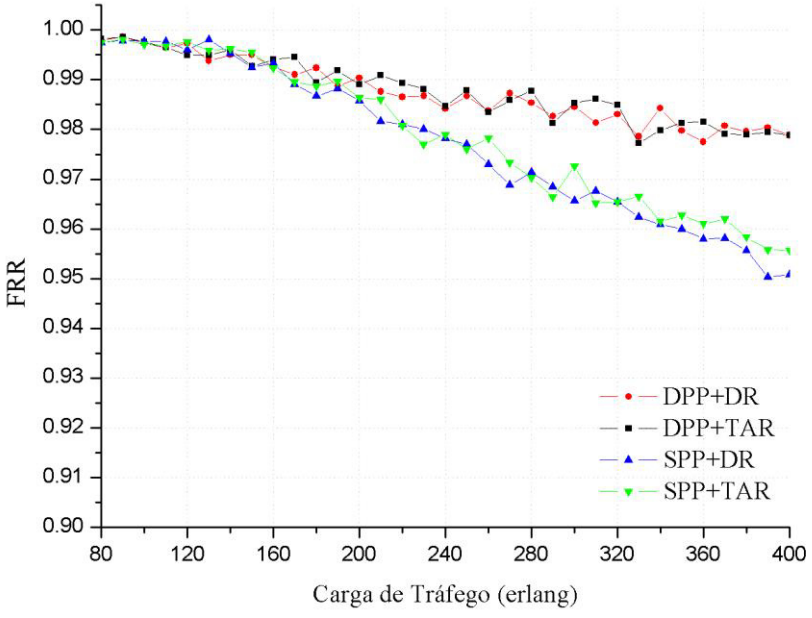
A magnitude das alterações das métricas depende da proporção de caminhos que são afetados e reestabelecidos. A diferença entre as amplitudes das curvas de FRR reflete diretamente nas demais métricas segundo o raciocínio apresentado. No entanto, as curvas SPP e DPP com TAR nos gráficos BP, SUR e AHOP não apresentam diferenças perceptíveis em relação às curvas SPP e DPP com DR. Como as curvas das métricas citadas apresentam correspondência com as curvas apresentadas no experimento da Seção 6.1.2, e as considerações realizadas anteriormente justificam esses resultados, elas foram disponibilizadas no Apêndice G: BP (Figura 81), SUR (Figura 82) e (Figura 83).

A métrica que nos resta analisar é a FRR (Figura 68). A primeira parte da análise é sobre as curvas DPP com a utilização do DR e do TAR. Observa-se que, em ambas as topologias, a utilização das restaurações produzem curvas de FRR semelhantes. Isso ocorre

porque os seus caminhos primários não concorrem na obtenção da proteção dos caminhos secundários, justamente por ser proteção dedicada, então a ordem em que as conexões são restauradas não influenciam no processo de restauração no esquema DPP. Na segunda parte da análise são comparadas as curvas SPP com a utilização do DR e do TAR. Nessas curvas, a amplitude da FRR do TAR apresenta uma suave elevação em relação ao DR, em ambas as topologias e em toda varredura de carga de tráfego. Segundo a **premissa 5**, a probabilidade de que ocorra uma alocação de caminho com granularidade fina de banda requerida é maior do que com granularidade grossa. Por isso, priorizar a recuperação das conexões com maior granularidade de banda requerida faz com que essas conexões garantam o seu reestabelecimento, deixando por último às conexões de granularidade fina que, de acordo com a lógica explicada, possuem maiores chances de que seus caminhos sejam alocados novamente. Assim, os caminhos compartilhados que concorrem entre si oferece prioridade na comutação para conexões com bandas de granularidade grossa que são menos prováveis de serem restabelecidos por restauração dinâmica. A proporção em que esses efeitos ocorrem é pequena, mas justificam essa diferença.



a)



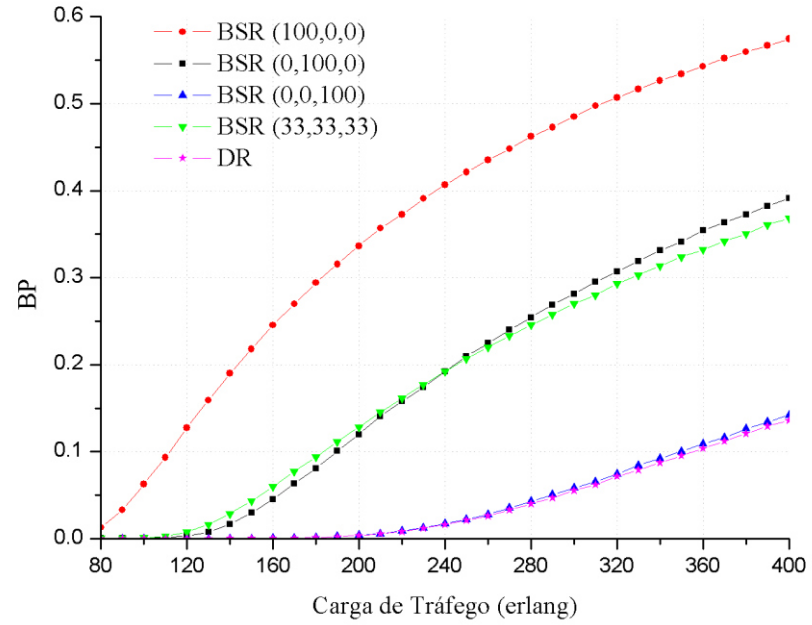
b)

Figura 68 - Gráfico de FRR comparando DR x TAR: a) NSFNET; b) USNET.

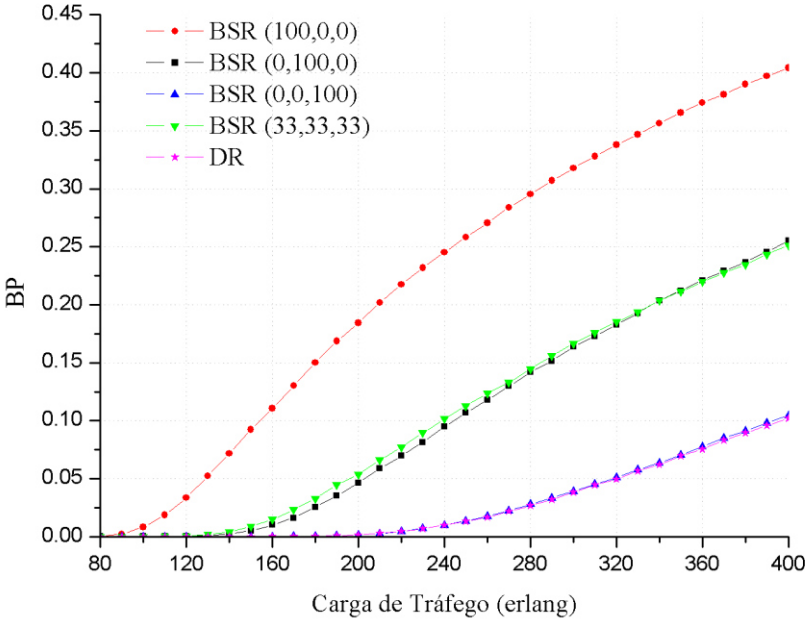
6.3 Resultados do Grupo 3 – BSR x DR

O BSR define três modelos de proteção e restauração baseadas nos níveis de serviço: FBGR, PBGR e BER. O primeiro modelo corresponde a uma DPP com restauração dinâmica padrão (DR). O segundo modelo é uma DPP parcial, ou seja, a banda alocada no caminho dedicado é reduzida em 50%, e com restauração dinâmica padrão. No último modelo não há proteção reservada, porém é executada uma restauração dinâmica com contração de banda, em que a banda pode ser reduzida até a mínima granularidade disponível. As conexões são geradas definindo-se as proporções de cada modelo apresentado. Em nossa notação, as proporções são dadas em porcentagens de 0 a 100, escritas entre parenteses e separadas por vírgula como no formato: "('FBGR','PBGR%','BER%')". As configurações definidas são (100,0,0), (0,100,0), (0,0,100), (33,33,34). Dos modelos dados, os que exibem a característica de contração de banda são o PBGR e o BER, sendo o primeiro com contração na proteção e o segundo na restauração. Como o modelo BER é desprovido de proteção, ele é comparado com as curvas obtidas apenas por restauração dinâmica padrão (DR). Sendo assim, a configuração BRS (100,0,0) e o DR formam os dois extremos de nosso experimento, um com 100% de proteção dedicada e outro sem proteção. As métricas utilizadas nesse experimento são: BP, SUR, AHOP, FRR.

Na métrica BP (Figura 69), em ambas as regiões de carga, a configuração BSR(100,0,0) é o que apresenta a maior BP. Como visto nos experimentos anteriores, o esquema DPP que constitui o BSR(100,0,0), consome um maior número de recursos para proteção e isso, consequentemente, aumenta a BP. No outro extremo de BP estão os esquemas BSR(0,0,100) e DR, que são desprovidos de proteção e, por isso, possuem as curvas mais baixas de BP. As curvas BSR(0,100,0) e BSR(33,33,33) possuem amplitudes intermediárias devido à proporção menor de banda requerida nos caminhos de proteção. A proporção de banda requerida para proteção em relação a banda requerida para os caminhos de trabalho no BSR(0,100,0) é 50% e no BSR(33,33,33) é 49,5%. Esta última é calculada pela expressão: $(1) \times 0{,}33 + (0.5) \times 0{,}33 + 0{,}33 \times (0) = 0{,}495$. Portanto, a proximidade de suas curvas de BP são coerentes com a quantidade de recursos demandados para proteção. Os desvios entre as curvas BSR(0,100,0) e BSR(33,33,33) são explicados pelos 33% de conexões que utilizam o modelo BER.



a)

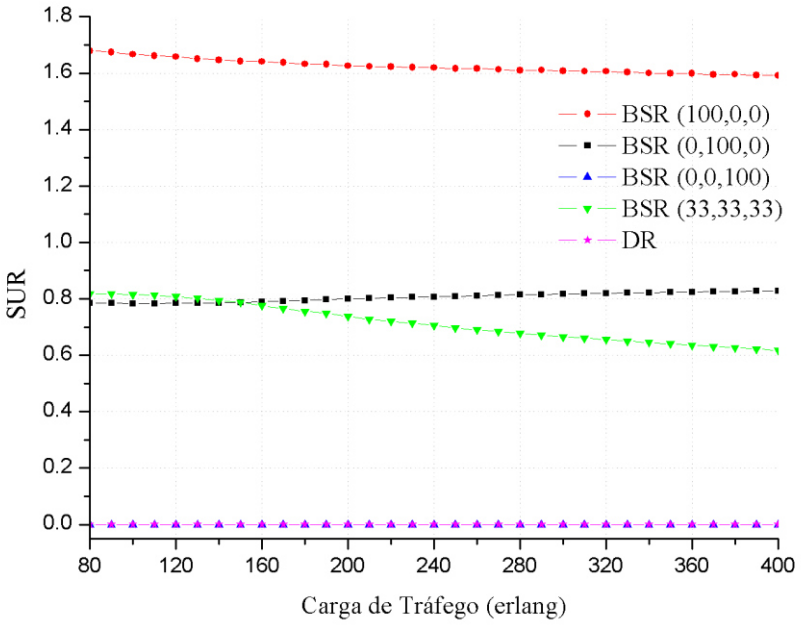


b)

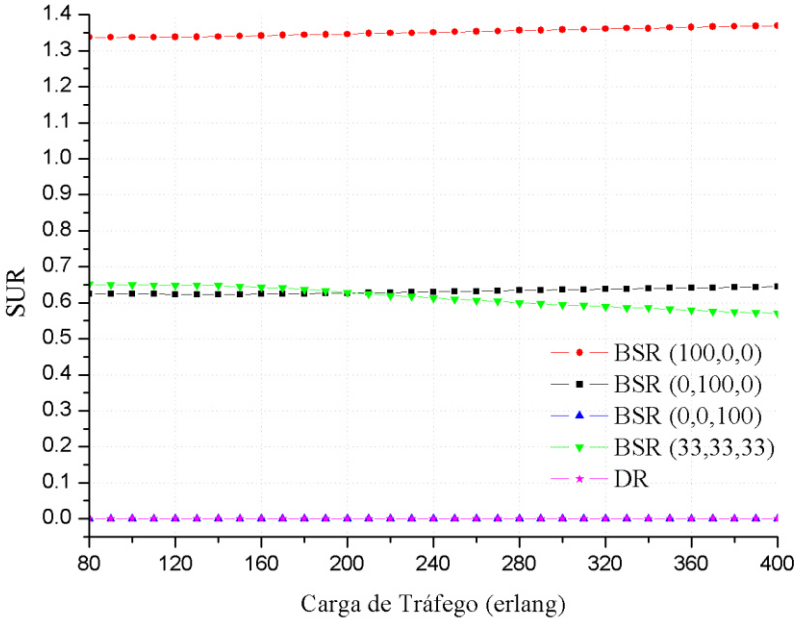
Figura 69 - Gráfico de BP comparando BSR x DR: a) NSFNET; b) USNET.

A métrica SUR é apresentada na Figura 70 e a quantidade total de recursos alocados pelos caminhos são mostrados na Tabela 18. Primeiramente, os dois extremos de SUR são dados pela configuração BSR(100,0,0), que apresenta maior amplitude, e pelas configurações BSR(0,0,100) e DR, que apresentam SUR igual a 0, pois ambas não alocam recursos para proteção (vide Tabela 18). Nas configurações intermediárias, BSR(0,100,0) e BR(33,33,33), observa-se que, na região de CB, as respectivas amplitudes são próximas entre si, e próximas da metade da amplitude de SUR da configuração BSR(100,0,0). Isso ocorre porque quase não há bloqueio de conexão nessa região, então as quantidades de recursos alocados para os caminhos primários das configurações BSR(100,0,0) BSR(0,100,0) e BSR(33,33,33) possuem valores próximos, como mostra a Tabela 18. Teoricamente, estima-se que a proporção da quantidade de recursos alocados para os caminhos de backup em relação aos recursos alocados para os caminhos primários era 50% para a configuração BSR(0,100,0) e 49,5% para a configuração BSR(33,33,33). Na Tabela 18, as quantidades de recursos alocados para os caminhos de backup são próximos do previsto.

Com o aumento da carga, a SUR da configuração BSR(33,33,33) decresce em relação à configuração BSR(0,100,0), para ambas as topologias. Nessa região, a SUR da configuração BSR(33,33,33) diminui porque a quantidade de recursos alocados pelos caminhos de trabalho aumenta devido à restauração por contração de banda dos 33% de conexões que implementam o modelo BER e a quantidade de recursos alocados pelos caminhos secundários diminui por causa da maior chance de bloqueio das conexões que implementam o modelo FBGR. Esta última afirmação é justificada pela **premissa 5.** As chances de bloqueio das conexões que implementam o modelo FBGR são maiores do que as conexões que implementam o PBGR. Dessa forma, a não alocação dessas conexões significa uma quantidade menor de recursos de proteção alocados.



a)



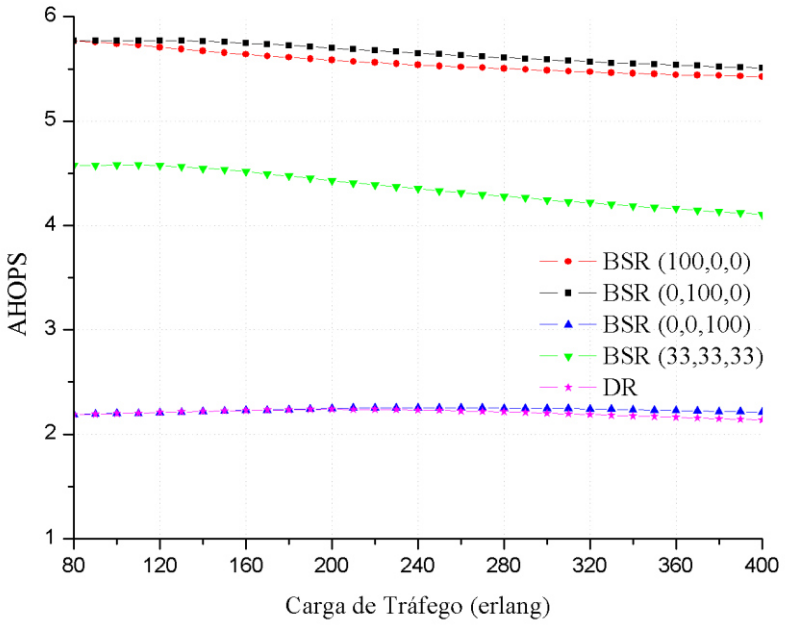
b)

Figura 70 - Gráfico de SUR comparando BSR x DR: a) NSFNET; b) USNET.

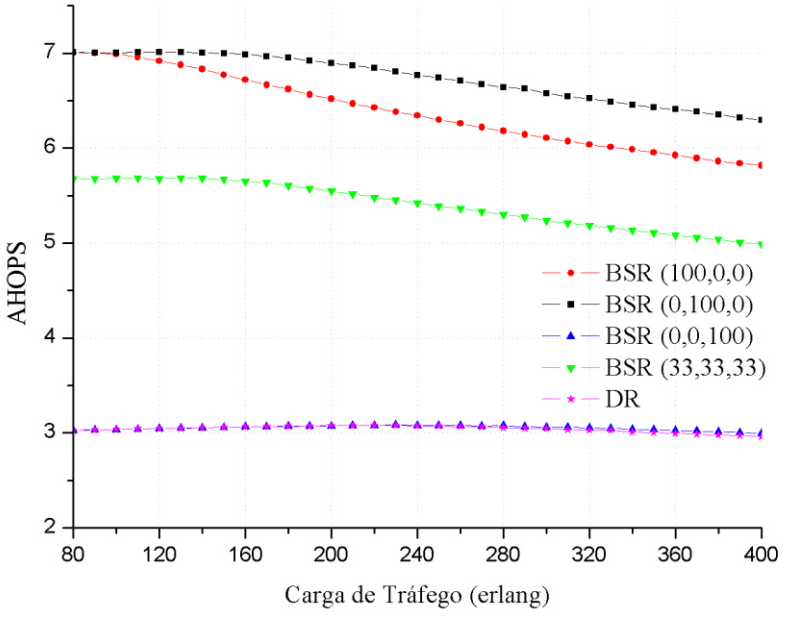
Tabela 18 - Quantidade total de recursos alocados para os esquemas com restauração BSR e DR

Curvas	Topologia	80 erlangs		240 erlangs		400 erlangs	
		Primário	Sec.	Primário	Sec.	Primário	Sec.
BRS(100,0,0)	NSFNET	12,722	21,355	6,920	11,206	4,724	7,518
BRS(0,100,0)		12,906	10,118	9,591	7,746	6,611	5,478
BRS(0,0,100)		13,126	0	13,153	0	10,768	0
BRS(33,33,33)		12,966	10,609	9,939	7,015	7,315	4,510
DR		13,127	0	13,104	0	10,734	0
BRS(100,0,0)	USNET	17,963	24,026	11,617	15,696	8,125	11,126
BRS(0,100,0)		17,995	11,234	15,283	9,637	11,172	7,204
BRS(0,0,100)		18,161	0	18,227	0	15,579	0
BRS(33,33,33)		18,041	11,74	15,331	9,398	11,598	6,629
DR		18,150	0	18,198	0	15,550	0

A métrica AHOP é apresentada na Figura 71. A configuração BSR(0,0,100) e o DR possuem baixo AHOP, pois eles não alocam caminhos secundários. As curvas com maiores AHOP correspondem às configurações BSR(0,100,0) e BSR(100,0,0). Entre elas, a configuração BSR(0,100,0) apresenta AHOP maior porque os caminhos secundários com menor banda requerida contribui para diminuição do bloqueio de caminhos mais longos. No patamar intermediário de AHOP está a curva da configuração BSR(33,33,33). Essa curva tem a sua média reduzida devido à parcela das conexões que utiliza o modelo BER, o qual não alocam caminhos secundários.



a)



b)

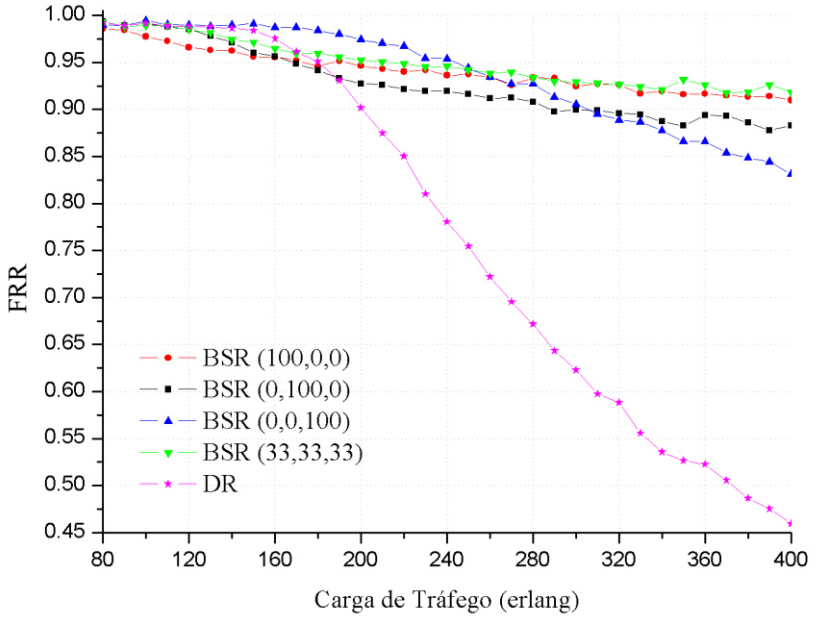
Figura 71 - Gráfico de AHOP comparando BSR x DR: a) NSFNET; b) USNET.

Por último, a análise da métrica FRR (Figura 72) toma como referências a configuração BSR(100,0,0) e o DR. Na região de CB, em ambas as topologias, todas as curvas de FRR situam-se próximas de 1. Nessa região, a disponibilidade de recursos é maior ainda para as curvas da configuração BSR(0,0,100) e do DR e, por isso, podem apresentar

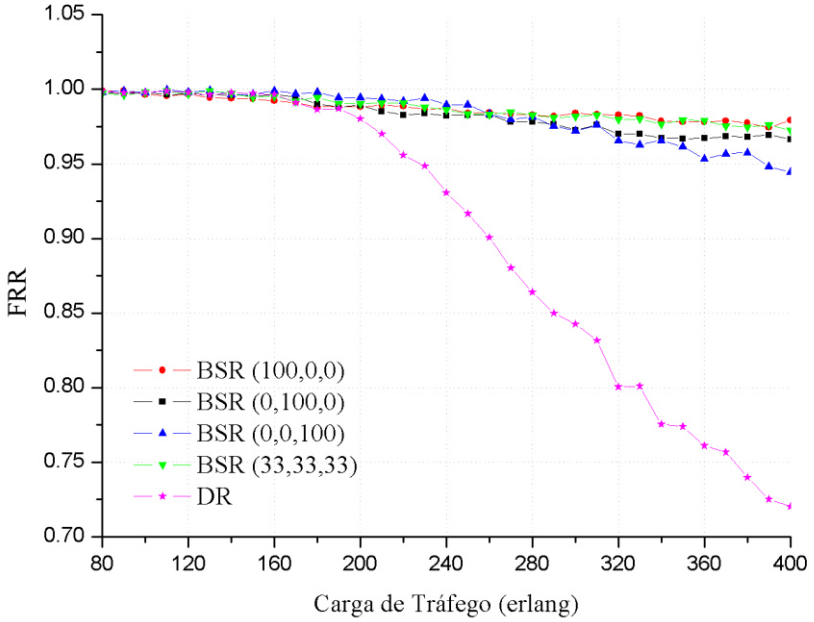
amplitudes de FRR maiores. Na região de CA, a curva DR apresenta declínio acentuado, indicando que a falta de uma proteção pré-reservada penaliza a recuperação das conexões afetadas. No entando, a configuração BSR(0,0,100), que implementa o modelo BER que também não tem proteção pré-reservada, apresenta uma FRR muito mais próxima de modelos com proteção do que com a DR. A capacidade de restauração dos caminhos de trabalho é melhor para o modelo BER do que o DR por causa da sua característica de contração que banda, que aumenta a possibilidade de alocação de um caminho, reduzindo a sua banda até a mínima granularidade (**premissa 5**).

As configurações que possuem algum tipo de proteção são as que apresentam maiores FRR, mesmo na região de CA. Considerando a curva da configuração BSR(100,0,0) como referência, a configuração BSR(33,33,33) apresenta uma FRR um pouco maior e a configuração BSR(0,100,0), menor. O resultado esperado em relação à configuração BSR(0,100,0) é que sua FRR deveria ser maior do que a da BSR(100,0,0) por causa da economia de espetro apresentada em sua SUR. Porém, existe um fator que não foi considerado nesse trabalho e que pode alterar a capacidade de estabelecimento de novos caminhos mesmo com economia de espectro, que é a fragmentação. O estabelecimento de um novo caminho depende da quantidade de slots de frequência livres, e também de como o conjunto de slots estão dispostos. Os caminhos alocados pelo esquema PBGR possui uma variação de granularidade maior do que o FBGR, e isso pode causar aumento da fragmentação do espectro.

Em relação à configuração BSR(33,33,33), o seu resultado superior pode ser explicado pela soma das seguintes contribuições: 1) menor fragmentação, porque o modelo PBGR é definido em menor proporção (33%); e 2) por apresentar 33% de BER, uma vez que este esquema possui alta restaurabilidade.



a)



b)

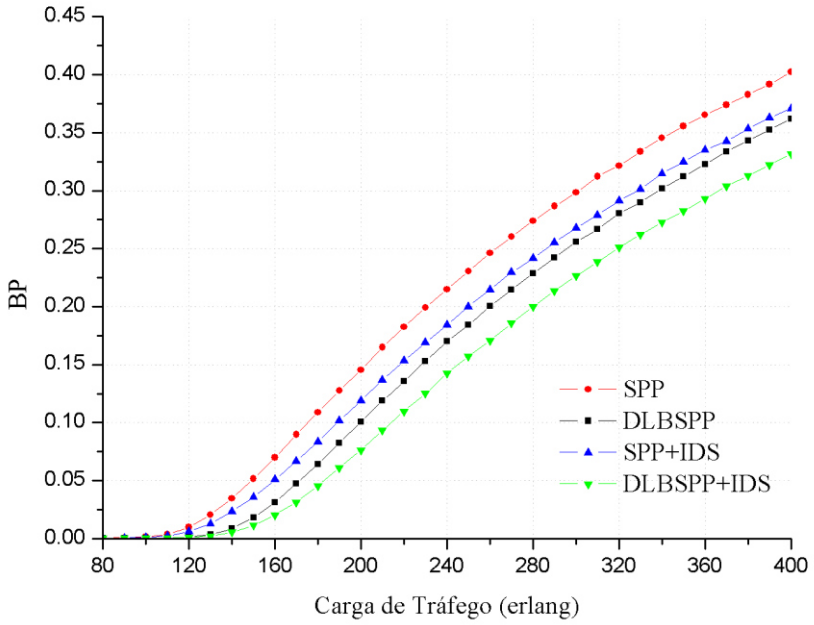
Figura 72 - Gráfico de FRR comparando BSR x DR: a) NSFNET; b) USNET.

6.4 Resultados do Grupo 4 – SPP x DLBSPP x SPP IDS x DLBSPP IDS com comutação de caminhos

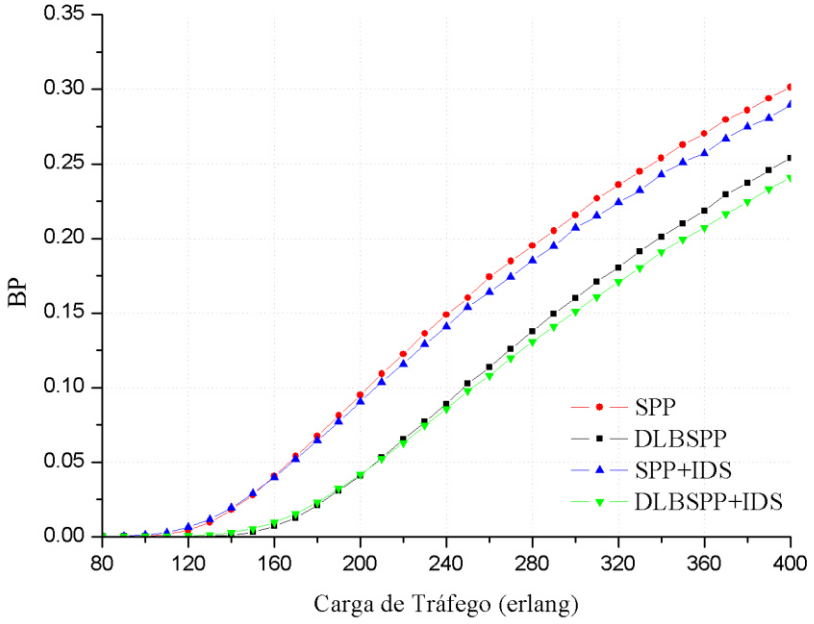
Nas simulações computacionais anteriores foram simulados os diferentes esquemas de proteção e restauração avaliados nesse trabalho. Nesse experimento, o esquema SPP é aplicado às heurísticas DLB (Seção 4.1.2) e IDS (Seção 4.2.2) e à combinação delas. Assim, foram obtidas as seguintes configurações: SPP, DLBSPP, SPP IDS e DLBSPP IDS. As métricas utilizadas nesse experimento são: BP, SUR, AHOP, *Primary* AHOP, *Backup* AHOP e FRR.

A primeira métrica é a BP, apresentada Figura 73. Considerando a curva SPP como referência, observa-se que o uso da heurística DLBSPP e IDS reduz a BP na maior parte da varredura de tráfego. O DLBSPP contribui para diminuição da BP porque permite encontrar caminhos primários com enlaces menos carregados (**premissa 1**) e, também, encontra caminhos secundários com enlaces menos carregados e com maior número de slots compartilhados, aumentando o número de compartilhamentos, resultando na diminuição da utilização do espectro (**premissa 4**). A heurística IDS permite que a alocação dos caminhos de proteção compartilhados tenda a ocorrer em uma região do espectro, evitando que alocações dos caminhos primários e secundários se intercalem. Dessa forma, o IDS permite que as alocações de recursos compartilhados convirjam para uma região, aumentando o nível de compartilhamento e, portanto, segundo a **premissa 4**, promovendo economia de espectro. A combinação das duas heurísticas produz menores BP em toda a faixa de tráfego, pois suas contribuições são somadas de maneira que o DLB escolhe os caminhos menos carregados e o IDS escolhe a região de alocação para obter máximo nível de compartilhamentos.

Apenas a curva SPP IDS apresenta uma BP maior do que a curva SPP, situada na região de CB na topologia USNET. Uma possível explicação é que a heurística IDS é sensível ao tamanho da topologia, ou seja, que as topologias de rede maiores reduzem a eficiência da heurística IDS, pois quanto maior a topologia de rede, maior é o número médio de hops de um caminho. Segundo a **premissa 6,** um maior número de hops aumenta a BP. Essa probabilidade é maior ainda ao se aplicar as restrições do esquema SPP.



a)



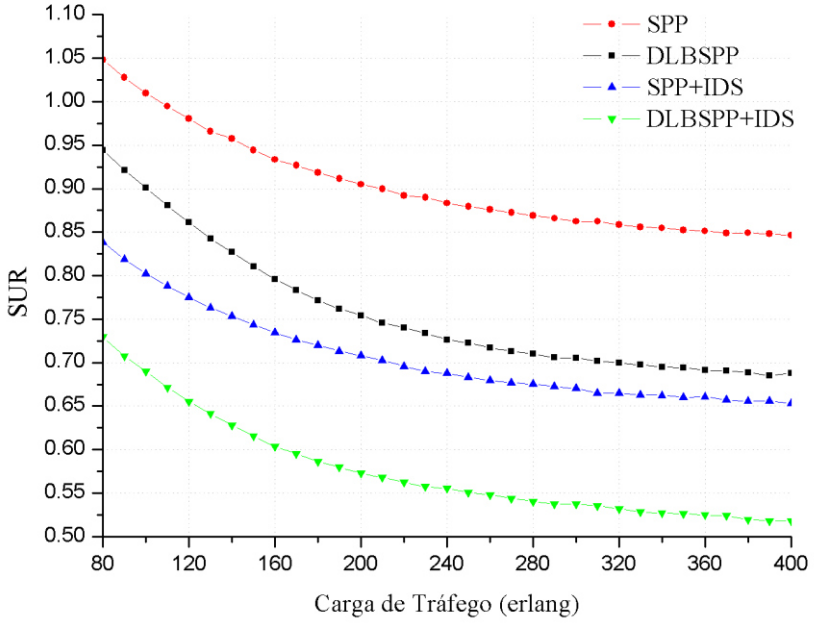
b)

Figura 73 - Gráfico de BP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET.

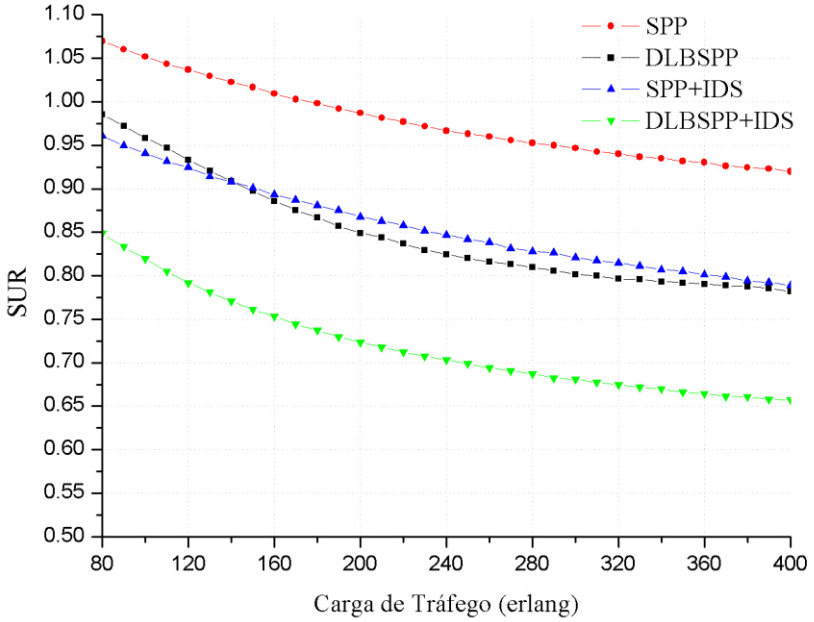
O nível de compartilhamento obtido pelas heurísticas reflete diretamente na métrica SUR (Figura 74). Em ambas as topologias, a menor SUR é obtida pelo esquema DLBSPP IDS. Dado a quantidade de recursos alocados pelos caminhos primários e de backup na

Tabela 19, observa-se que a combinação das contribuições de cada heurística (DLB+IDS) permite reduzir a quantidade de recursos alocados para os caminhos de proteção compartilhados ao mesmo tempo em que aumenta a alocação de caminhos primários.

O IDS promove uma SUR menor do que o DLBSPP na topologia NSFNET (Fig.74a) em toda a faixa de tráfego. Na topologia USNET (Fig.74b) o IDS é inferior ao DBLSPP apenas na região de CB, mas no restante da faixa de carga de tráfego o DLBSPP apresenta uma SUR menor. Observa-se que mesmo o SPP IDS apresentando uma SUR menor do que o DLBSPP na topologia NSFNET, ele apresenta uma BP maior. Por outro lado, na topologia USNET, especificamente na região de CA, a SUR do SPP IDS é um pouco maior do que o DLBSPP, no entanto, a redução relativa de BP em 400 *erlangs* promovida pelo DLBSPP é $-15{,}74\%$ contra $-3{,}94\%$ do SPP IDS. A redução de BP ocorre porque o efeito economia de espectro supera na maior parte da varredura de tráfego o efeito contrário das restrições impostas pelo compartilhamento de recursos. Esse fato ajuda a sustentar a tese de que o IDS é sensível ao tamanho da rede.



a)



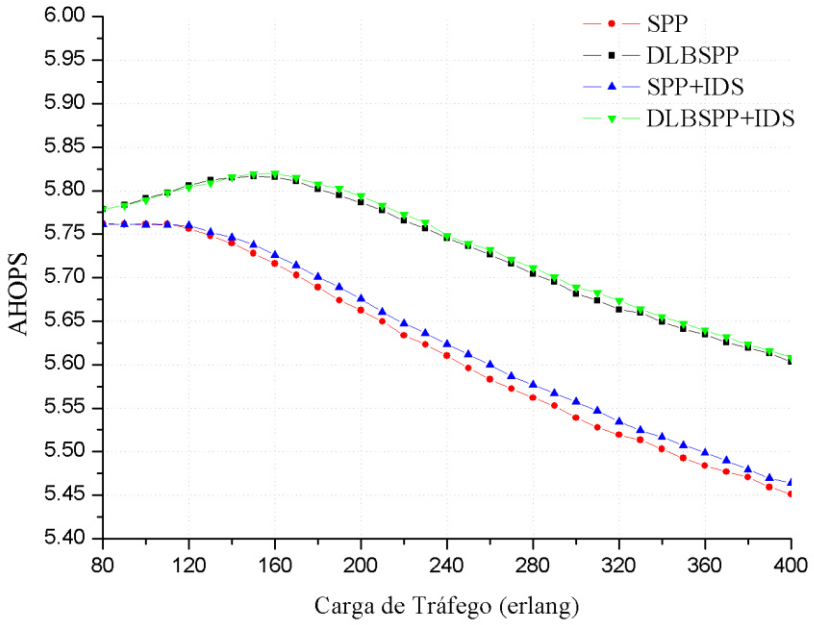
b)

Figura 74 - Gráfico de SUR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET.

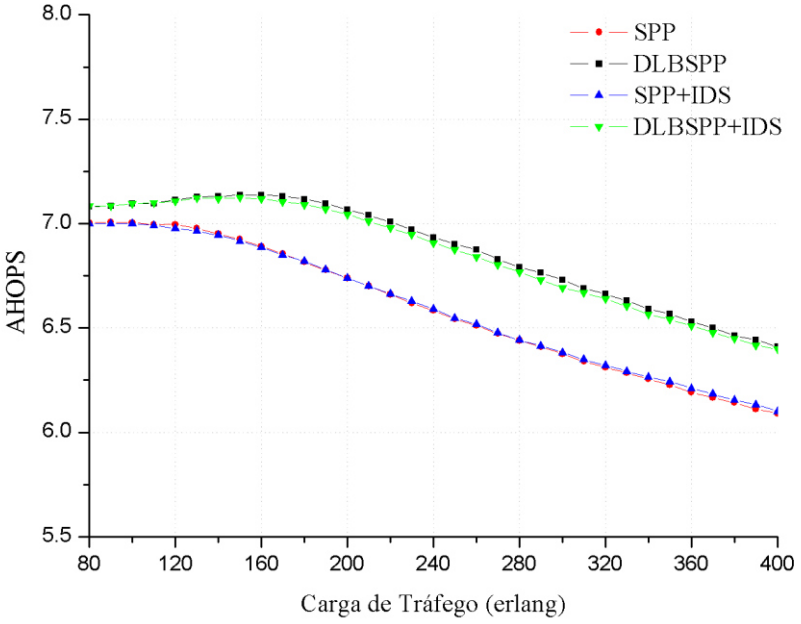
Tabela 19 - Quantidade total de recursos alocados para os esquemas SPP, DLBSPP, SPP IDS e DLBSPP IDS (x 1 milhão).

Curvas	Topologia	80 erlangs		240 erlangs		400 erlangs	
		Primário	Sec.	Primário	Sec.	Primário	Sec.
SPP	NSFNET	12,855	13,473	9,116	8,051	6,278	5,315
DLBSPP	NSFNET	12,870	12,157	10,106	7,340	6,987	4,807
SPP IDS	NSFNET	12,847	10,771	9,571	6,582	6,666	4,354
DLBSPP IDS	NSFNET	12,859	9,384	10,444	5,801	7,321	3,793
SPP	USNET	17,956	19,207	13,772	13,309	10,046	9,243
DLBSPP	USNET	17,978	17,713	15,625	12,887	11,302	8,835
SPP IDS	USNET	17,940	17,239	13,938	11,803	10,259	8,096
DLBSPP IDS	USNET	17,965	15,249	15,558	10,942	11,455	7,526

A métrica seguinte, AHOP (Figura 75), mostra uma característica fundamental do uso da heurística DLBSPP: alterar o objetivo do roteamento. No DLBSPP, os valores de custo dos enlaces são ponderados em função da disponibilidade de recursos e número de slots compartilhados. Dessa forma, o algoritmo *Dijkstra* encontra menor caminho em custo e não necessariamente o menor caminho em número de hops, resultando em caminhos que podem ser mais longos para atender as funções de balanceamento. O resultado mostra que as curvas de AHOP com uso do balanceamento de carga, DLBSPP e DLBSPP IDS, são maiores do que as que utilizam o roteamento tradicional, inclusive nas suas componentes *Primary* AHOP (Figura 76) e *Backup* AHOP (Figura 77). De acordo com **a premissa 6**, a BP de conexões com caminhos mais longos é maior, porém, o uso da heurística DLB obriga que os enlaces selecionados sejam menos carregados aumentando a probabilidade de alocação (**premissa 1**). Consequentemente, aumenta a probabilidade de alocação de conexões com caminhos mais longos, aumentando o AHOP. No IDS, devido ao aumento do número de compartilhamentos e menor BP o AHOP aumenta.

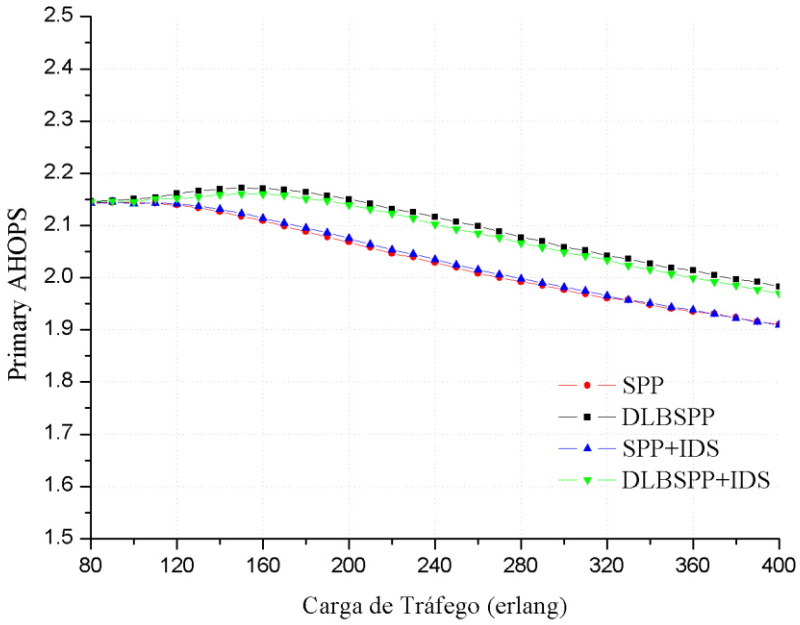


a)

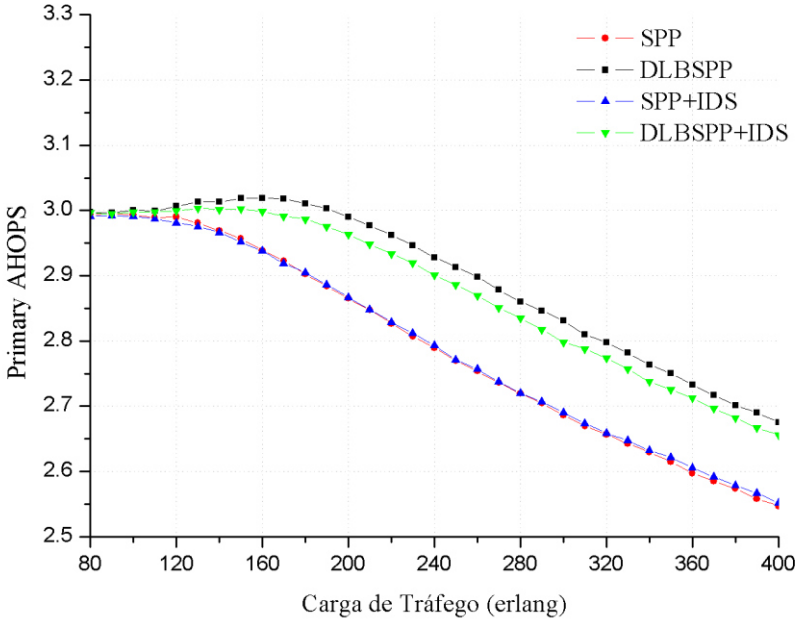


b)

Figura 75 - Gráfico de AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET.

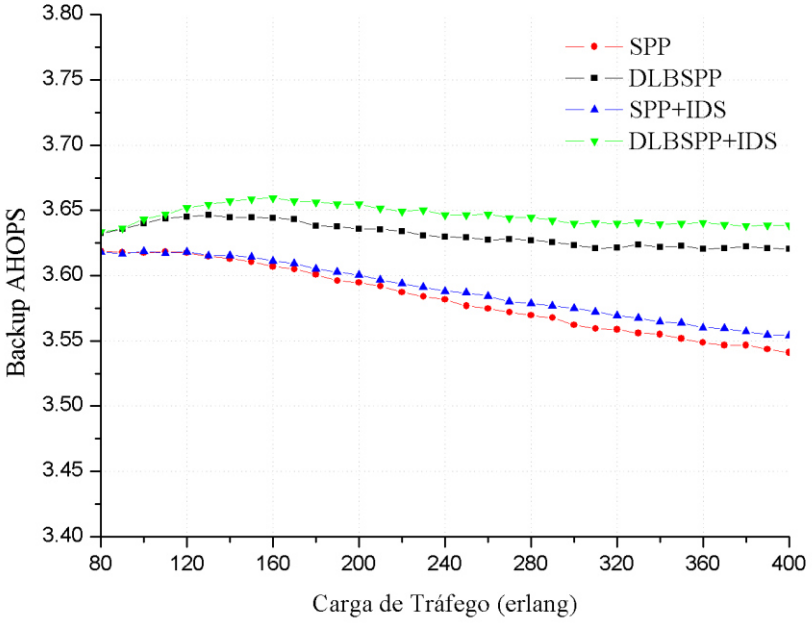


a)

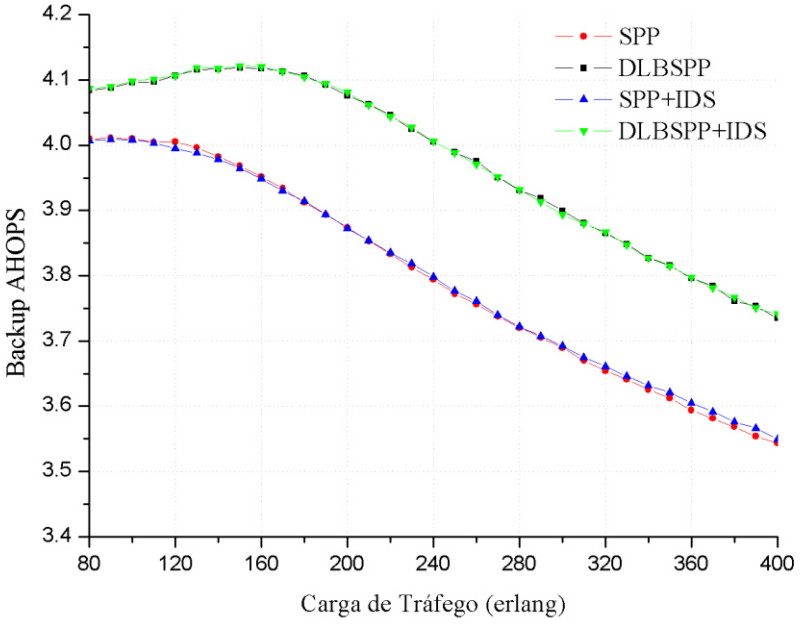


b)

Figura 76 - Gráfico de *Primary* AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET.



a)

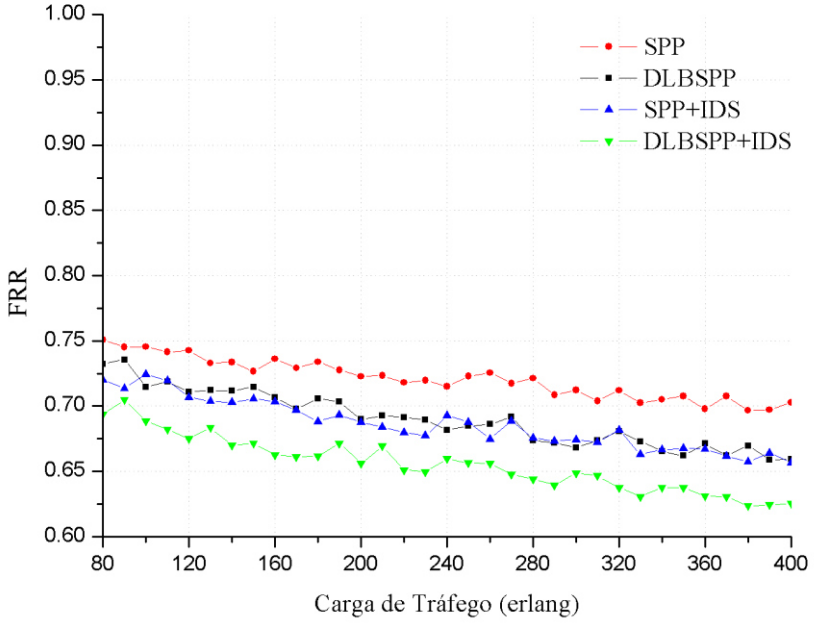


b)

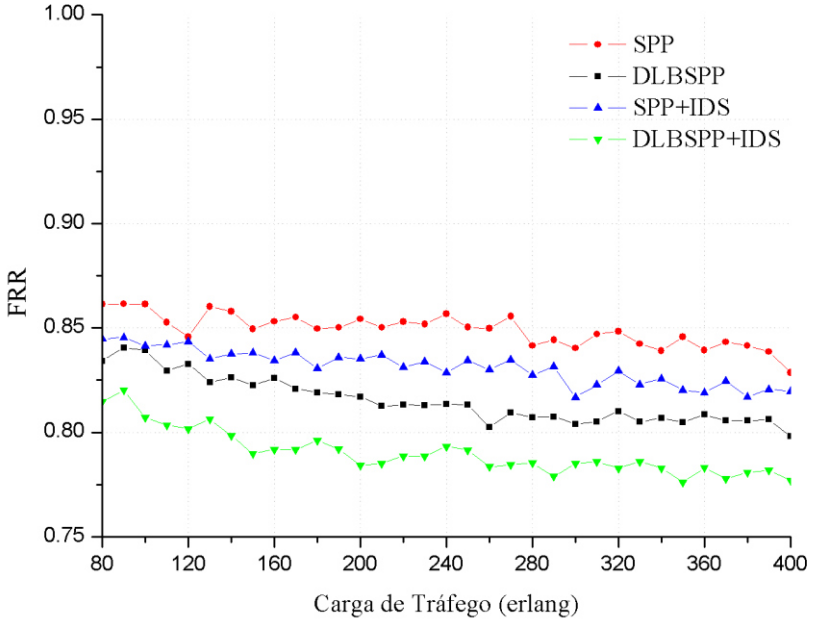
Figura 77 - Gráfico de *Backup* AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET.

Por último, a métrica FRR é apresentada na Figura 78. Primeiramente, considerando a curva SPP como referência, observa-se que todas as curvas apresentam FRR menor. Isso acontece porque as heurísticas utilizadas aumentam o número de compartilhamentos e, de acordo a análise realizada na Seção 6.1.2, quanto maior o número de compartilhamentos maior o nível de comprometimento das conexões que implementam o esquema SPP.

Nesse resultado, não se pode comparar diretamente as curvas DLBSPP e o SPP IDS, porém é possível considerar as contribuições de cada uma separadamente. A heurística DLB provoca um primeiro nível de redução da FRR. Ao aplicar a heurística IDS, os esquemas SPP e DLBSPP apresentam outro nível de redução. A combinação DLBSPP IDS é a curva que possui menor FRR devido à soma das contribuições de cada heurística.



a)



b)

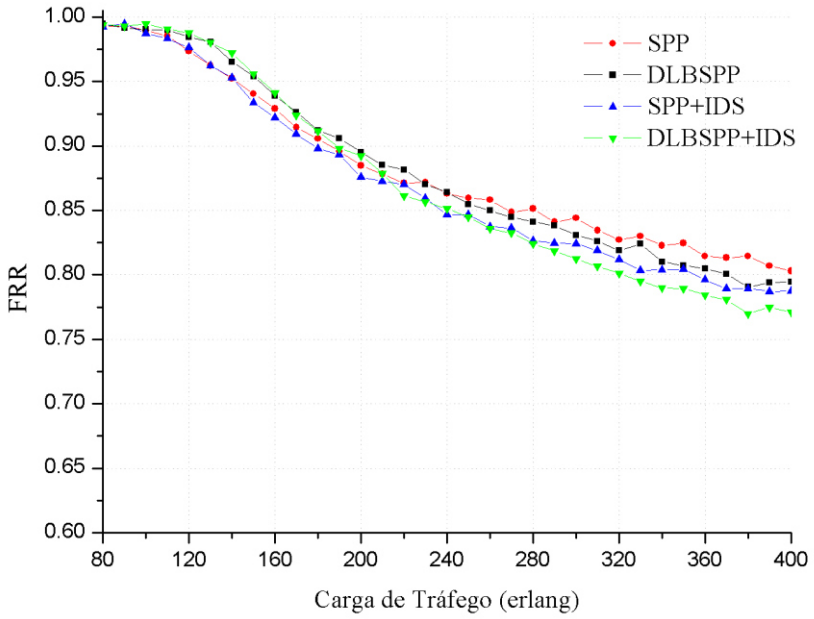
Figura 78 - Gráfico de FRR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS sem restauração dinâmica: a) NSFNET; b) USNET.

6.5 Resultados do Grupo 5 – SPP x DLBSPP x SPP IDS x DLBSPP IDS com restauração dinâmica

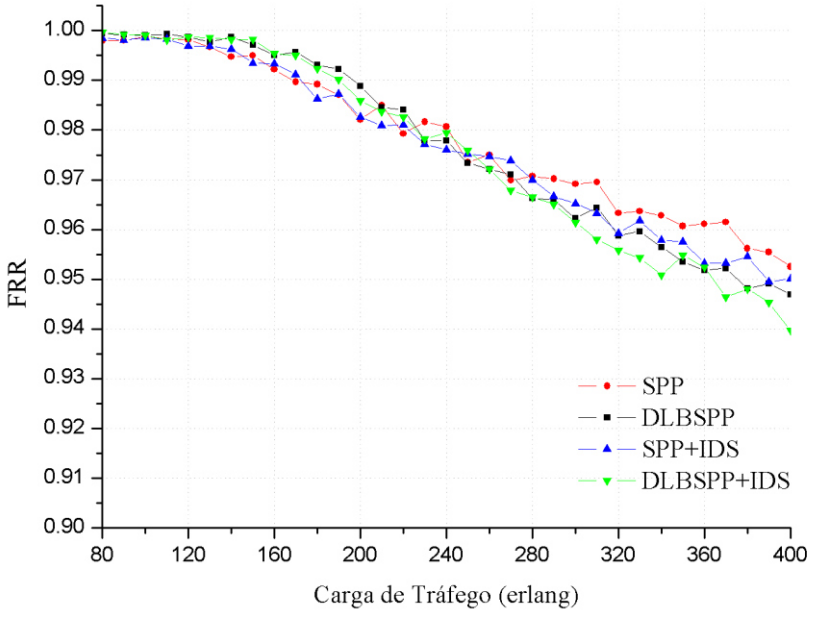
Esse experimento reproduz as mesmas configurações do Grupo 4 e implementa a restauração dinâmica nos casos em que a recuperação por comutação de caminhos falham. As métricas utilizadas são: BP, SUR, AHOP, FRR.

Os resultados obtidos para este experimento apresentaram curvas semelhantes aos resultados do experimento do Grupo 4 porque, neste caso, a influência da restauração dinâmica sobre demais métricas é insignificante. Sendo assim, os seguintes gráficos podem ser consultados no Apêndice H: BP (Figura 84), SUR (Figura 85), AHOP (Figura 86).

Dado o exposto, a métrica que resta analisar é a FRR apresentada na Figura 79. Utilizando a curva SPP como referência, observa-se que as curvas estão dispostas na mesma ordem em que as suas variações heurísticas apresentada na Seção 6.4. No entanto, observa-se também que as diferenças entre as curvas são bem mais estreitas. Isso ocorre porque a restauração dinâmica utilizada com combinações heurísticas compensam as deficiências provocadas pelo maior nível de compartilhamento (comprometimento das conexões). A Tabela 20 apresenta o ganho relativo de FRR com a presença da restauração dinâmica entre os esquemas SPP, DLBSPP, SPP IDS e DLBSPP IDS. O ganho relativo obtido pela heurística DLB é maior do que a heurística IDS e a combinação de DLBSPP IDS é maior que ambos. Observa-se que a combinação dos efeitos das heurísticas promove maior capacidade de restauração dinâmica.



a)



b)

Figura 79 - Gráfico de FRR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET.

Tabela 20 - Ganho relativo percentual de FRR entre os esquemas SPP, DLBSPP, SPP IDS e DLBSPP IDS.

Esquema	Topologia	80 erlangs	240 erlangs	400 erlangs
SPP	NSFNET	32,22%	20,73%	14,25%
DLBSPP		35,83%	26,77%	20,52%
SPP IDS		37,81%	22,17%	19,88%
DLBSPP IDS		43,26%	29,01%	23,28%
SPP	USNET	15,83%	14,47%	14,26%
DLBSPP		19,80%	20,22%	18,64%
SPP IDS		18,19%	17,80%	15,89%
DLBSPP IDS		22,70%	23,48%	20,95%

7 CONCLUSÕES

O aumento crescente da demanda por largura de banda tem motivado o desenvolvimento de tecnologias para redes ópticas para transmitirem a taxas de 400 G até 1 Tb/s por canal. As redes ópticas atualmente implantadas, cujas taxas de transmissão são de 40 e 100 Gb/s por canal, operam com grade fixa de frequências, e a atualização para taxas de 400 G até 1 T acarretam problemas de escalabilidade e flexibilidade. Nesse contexto, a arquitetura EON foi apresentada como uma das tecnologias promissoras para a próxima geração de redes ópticas. A EON utiliza técnicas de transmissão multiportadoras, como o O-OFDM e filtragem de Nyquist, que geram subportadoras ortogonais e formam uma grade espectral granular e flexível, sendo capaz de alocar recursos espectrais necessários de acordo com a demanda de tráfego, promovendo eficiência espectral e elasticidade.

Devido ao aumento significativo da taxa de transmissão, falhas nos componentes de rede (nos nós ou enlaces) podem acarretar a interrupção de múltiplos canais de serviços e uma grande perda de dados. Diante desse cenário de falha, é necessário que haja mecanismos que contornem o problema até que os componentes de rede sejam reparados pelos operadores de rede. A sobrevivência das conexões afetadas por falhas é garantida pelos esquemas de proteção e restauração implementados no plano de controle da rede. O plano de controle é um sistema autônomo, composto por um conjunto de protocolos, que permite detectar uma ocorrência falha e acionar os esquemas de proteção e restauração necessários para o restabelecimento da conexão do usuário de forma transparente.

O estudo conduzido neste trabalho aborda a análise de desempenho de alguns esquemas de proteção recentes voltados a redes elásticas como: SPP ASP, DLBSPP e o BSR. O SPP ASP é uma implementação de SPP para redes EONs que compartilha individualmente os slots de frequência do espectro granular. Esta implementação é utilizada para o DLBSPP, que utiliza métricas heurísticas para balanceamento de carga nos enlaces na computação dos caminhos primários e de proteção compartilhados. E, por último, o esquema BSR, que utiliza diferentes níveis de proteção baseados no DPP de acordo níveis de serviço de cada conexão. No que concerne ao esquema SPP, foi aplicada também a heurística de alocação IDS, que escolhe regiões de alocação diferentes para os caminhos primários e de proteção compartilhados. Independentemente do tipo de proteção utilizado, a restauração é realizada em dois passos, primeiro por comutação de caminhos e em seguida por restauração dinâmica. A restauração dinâmica utiliza a combinação dos algoritmos *Dijkstra+first-fit* como solução

base para resolver separadamente os subproblemas de roteamento e alocação de espectro, respectivamente, sendo essa a mesma base utilizada para alocação dos caminhos primários e secundários das conexões.

Os esquemas de proteção e restauração estudados foram simulados e divididos em cinco grupos de comparação. Na primeira parte do experimento do Grupo 1, foi analisado o desempenho dos esquemas SPP e DPP com e sem restauração dinâmica para o caso de uma única falha. Os resultados obtidos mostram que o SPP garante a mesma capacidade de restauração do DPP usando apenas a comutação de caminhos, dispensando o uso da restauração dinâmica, e apresenta probabilidade de bloqueio menor do que o DPP devido a sua capacidade de compartilhamento de recursos. Em uma rede real, em que a disponibilidade dos equipamentos de redes é maior do que 0,99, a probabilidade de ocorrer múltiplas falhas é baixa e, por isso, a melhor solução de proteção de rede para o cenário de uma única falha é a utilização do esquema SPP. Na segunda parte do experimento do Grupo 1, assumimos um cenário de múltiplas falhas, e foi concluído que a taxa de restauração do SPP é mais comprometida do que a do DPP devido à dependência entre os caminhos de trabalho e caminhos compartilhados. Neste caso, o uso da restauração dinâmica fez com que a taxa de restauração do esquema SPP fosse maior do que o DPP na região de baixa carga de tráfego. Por outro lado, na região de alta carga de tráfego, a taxa de restauração do SPP apresentou um desempenho menor do que o DPP. Apesar ter apresentado uma menor taxa de restauração na região de alta carga de tráfego, o esquema SPP ainda obteve uma probabilidade de bloqueio bem mais baixa do que o DPP. Sendo assim, concluímos que para a maioria dos casos, o esquema SPP é mais vantajoso do que o DPP.

No experimento do Grupo 2 foi comparada a restauração padrão com a restauração TAR. Os resultados obtidos para os dois tipos de restauração no esquema DPP foram praticamente idênticos. Isso acontece porque a ordenação proposta pelo TAR não afeta o DPP, pois em nenhum momento os caminhos de trabalho concorrem entre si pela proteção. Por outro lado, para o esquema SPP, o TAR apresentou uma taxa de restauração um pouco melhor do que a restauração dinâmica padrão.

No experimento do Grupo 3, vimos que as conexões que usam esquema FBGR consomem muitos recursos e tem uma probabilidade de bloqueio alta. O esquema PBGR apresenta um consumo de recursos e probabilidade de bloqueio intermediário, porém ele provoca maior fragmentação no espetro e isso prejudica na restauração dinâmica. A BER não consome recursos de backup e por isso proporciona baixa probabilidade de bloqueio e utilização de espectro. Por outro lado, devido a técnica de contração de banda, a BER

consegue flexibilizar as restrições de banda requerida e aumentar consideravelmente a taxa de restauração.

Os esquemas BSR não podem ser arbitrariamente configurados pelo operador de rede, porque dependem do tipo de nível de serviço associado às conexões de entrada. Como as proporções dos níveis de serviço das conexões de entrada podem variar de maneira aleatória e proporcionar inúmeras combinações, não é possível concluir qual é o melhor esquema em todas as situações. Esse experimento abordou quatro configurações distintas, sendo que a configuração que mostrou pior desempenho foi a que teve maior proporção do esquema PBGR. O PBGR permite alocar menores bandas nos caminhos de proteção e isso aumenta o diferencial de largura de banda alocada e que acarreta um problema de fragmentação de espectro. Esse problema necessita de mais estudos para avaliá-lo. Uma medida alternativa para contorná-lo seria utilizar um algoritmo de decisão para substituir o esquema PBGR pelo FBGR ou BER.

Os experimentos do Grupo 4 e Grupo 5 testaram as diferentes combinações heurísticas para o esquema SPP. Nos resultados obtidos no experimento do Grupo 4 vimos que as heurísticas expressam uma relação de compromisso, que diminui a probabilidade de bloqueio e utilização do espectro devido ao aumento do número de compartilhamentos em troca de uma menor taxa de restauração. Ou seja, as heurísticas permitem aumentar o nível de compartilhamento e isso implica diminuição da probabilidade de bloqueio e da taxa de restauração. No experimento do Grupo 5, foi acrescentado o processo de restauração dinâmica. Os resultados obtidos demostraram as vantagens do uso da restauração dinâmica, principalmente com uso das heurísticas. Neste experimento observou-se que ainda existe a relação de compromisso “probabilidade de bloqueio” e “taxa de restauração”, porém, os resultados mostraram que a redução da probabilidade de bloqueio é mais acentuada do que a sua respectiva redução na taxa de restauração. Na topologia de rede USNET, a variação da taxa de restauração é mínima e, por isso, o DLBSPP IDS é a melhor opção, já que apresenta probabilidade de bloqueio menor do que as outras. Na topologia NSFNET, por ser uma topologia menor, é possível visualizar as diferenças entre as curvas de taxa de restauração dos esquemas heurísticos propostos.

Sugerimos para trabalho futuro testar o esquema BSR com base no esquema SPP. Outra sugestão é criar heurísticas para o SPP que realizam uma função de roteamento para: 1) distribuir o risco de comprometimento para diminuir as penalidades no processo de restauração por comutação de caminhos e; 2) considerar o tamanho das pilhas de alocação compartilhadas criadas pelo IDS para evitar caminhos que permitem a sua expansão para área

de alocação dos caminhos primários. No processo de alocação de espectro há campo de estudo para o desenvolvimento de uma heurística que avalie a melhor solução factível que promova menor fragmentação futura.

REFERÊNCIAS

[1] E. Pincemin, M. Song, Y. Loussouarn, G. Thouenon, and C. Betoule, "Towards 400G/1T flexible optical transport networks," in *Transparent Optical Networks (ICTON), 2013 15th International Conference on*, 2013, pp. 1-13.

[2] Cisco, "Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper", 2015. [Online]. Disponível em: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html. [Acesso em: 08- Jan- 2016].

[3] M. Jinno, H. Takara, B. Kozicki, Y. Tsukishima, Y. Sone, and S. Matsuoka, "Spectrum-Efficient and Scalable Elastic Optical Path Network: Architecture, Benefits, and Enabling Technologies," *Ieee Communications Magazine,* vol. 47, pp. 66-73, Nov 2009.

[4] A. S. Tanenbaum and D. Wetherall, *Computer Networks*, 5th ed.: Pearson Prentice Hall, 2011.

[5] K. Christodoulopoulos, I. Tomkos, and E. A. Varvarigos, "Elastic Bandwidth Allocation in Flexible OFDM-Based Optical Networks," *Journal of Lightwave Technology,* vol. 29, pp. 1354-1366, 2011.

[6] Y. Wang, X. Cao, and Y. Pan, "A Study of the Routing and Spectrum Allocation in Spectrum-sliced Elastic Optical Path Networks," *2011 Proceedings Ieee Infocom,* pp. 1503-1511, 2011.

[7] A. N. Patel, P. N. Ji, J. P. Jue, and T. Wang, "Routing,Wavelength Assignment, and Spectrum Allocation in Wavelength-Convertible Flexible Optical WDM (WC-FWDM) Networks," in *National Fiber Optic Engineers Conference*, Los Angeles, California, 2012, p. JTh2A.36.

[8] B. Chen, J. Zhang, Y. Zhao, C. Lv, W. Zhang, S. Huang*, et al.*, "Multi-link failure restoration with dynamic load balancing in spectrum-elastic optical path networks," *Optical Fiber Technology,* vol. 18, pp. 21-28, Jan 2012.

[9] Y. Sone, A. Watanabe, W. Imajuku, Y. Tsukishima, B. Kozicki, H. Takara*, et al.*, "Highly Survivable Restoration Scheme Employing Optical Bandwidth Squeezing in Spectrum-Sliced Elastic Optical Path (SLICE) Network," *Conference on Optical Fiber Communication,* vol. 1-5, pp. 1626-1628, 2009.

[10] Y. Sone, A. Watanabe, W. Imajuku, Y. Tsukishima, B. Kozicki, H. Takara*, et al.*, "Bandwidth Squeezed Restoration in Spectrum-Sliced Elastic Optical Path Networks (SLICE)," *Journal of Optical Communications and Networking,* vol. 3, pp. 223-233, 2011.

[11] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *Lightwave Technology, Journal of,* vol. 21, pp. 870-883, 2003.

[12] X. Shao, Y.-K. Yeo, Z. Xu, X. Cheng, and L. Zhou, "Shared-Path Protection in OFDM-based Optical Networks with Elastic Bandwidth Allocation," in *Optical Fiber Communication Conference*, 2012, p. OTh4B.4.

[13] ITU-T, "G.694.1 - Spectral grids for WDM applications: DWDM frequency grid", 2012. [Online]. Disponível em: http://www.itu.int/rec/T-REC-G.694.1-201202-I/en. [Acesso em: 09- Jan- 2016].

[14] O. Gerstel, M. Jinno, A. Lord, and S. J. B. Yoo, "Elastic optical networking: a new dawn for the optical layer?," *Communications Magazine, IEEE,* vol. 50, pp. s12-s20, 2012.

[15] R. Schmogrow, M. Winter, M. Meyer, D. Hillerkuss, S. Wolf, B. Baeuerle*, et al.*, "Real-time Nyquist pulse generation beyond 100 Gbit/s and its relation to OFDM," *Optics Express,* vol. 20, pp. 317-337, 2012.

[16] P. B. Osgood, *Lecture Notes for EE 261 the Fourier Transform and Its Applications*: CreateSpace Independent Publishing Platform, 2014.

[17] Teleco, "Redes WDM: Equipamentos", 2012. [Online]. Disponível em: http://www.teleco.com.br/tutoriais/tutorialrwdm/pagina_3.asp. [Acesso em: 09- Jan- 2016].

[18] Fiberstore Team, "Fiber Optic Transponders Tutorial", *Fiberstore*, 2015. [Online]. Disponível em: http://www.fs.com/fiber-optic-transponders-tutorial-aid-453.html. [Acesso em: 09- Jan- 2016].

[19] N. Sambo, P. Castoldi, A. D'Errico, E. Riccardi, A. Pagano, M. S. Moreolo*, et al.*, "Next generation sliceable bandwidth variable transponders," *Communications Magazine, IEEE,* vol. 53, pp. 163-171, 2015.

[20] J. Emerson, "Add/Drop Regenerator Multiplexer System (ADR)", *Fiberdyne*, 2009. [Online]. Disponível em: http://www.fiberdyne.com/products/add-drop-regen-multiplexer.html. [Acesso em: 09- Jan- 2016].

[21] Enablence, "The Next Generation ROADM Network", 2010. [Online]. Disponível em: http://www.enablence.com/thinking-innovation/40g-100g-metro-networks/nextgen-roadm-network. [Acesso em: 10- Jan- 2016].

[22] L. Eldada, "Advances in ROADM technologies and subsystems," 2005, pp. 597022-597022-10.

[23] M. Sharma and G. Cohen, "Wavelength selective switch," ed: Google Patents, 2014.

[24] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Algoritmos: teoria e prática*, 2ª ed.: CAMPUS - RJ, 2002.

[25] M. N. Ellanti, *Next Generation Transport Networks: Data, Management, and Control Planes*: Springer, 2005.

[26] J. Sócrates-Dantas, D. Careglio, J. Perelló, R. M. Silveira, W. V. Ruggiero, and J. Solè-Pareta, "Challenges and requirements of a control plane for elastic optical networks," *Computer Networks,* vol. 72, pp. 156-171, 10/29/ 2014.

[27] G. Li, J. Yates, D. Wang, and C. Kalmanek, "Control plane design for reliable optical networks," *Communications Magazine, IEEE,* vol. 40, pp. 90-96, 2002.

[28] P. Ji, Z. Ge, J. Kurose, and D. F. Towsley, "A comparison of hard-state and soft-state signaling protocols," *IEEE/ACM Transactions on Networking,* vol. 15, pp. 281-294, 2007.

[29] D. C. Kilper, R. Bach, D. J. Blumenthal, D. Einstein, T. Landolsi, L. Ostar*, et al.*, "Optical performance monitoring," *Lightwave Technology, Journal of,* vol. 22, pp. 294-304, 2004.

[30] J. M. Kahn and H. Keang-Po, "Spectral efficiency limits and modulation/detection techniques for DWDM systems," *Selected Topics in Quantum Electronics, IEEE Journal of,* vol. 10, pp. 259-272, 2004.

[31] P. J. Winzer, "High-Spectral-Efficiency Optical Modulation Formats," *Lightwave Technology, Journal of,* vol. 30, pp. 3824-3835, 2012.

[32] Z. Chunlei, Z. Pengtu, and G. Ling, "A survey of advanced modulation formats for high-speed transmission," in *Computer Application and System Modeling (ICCASM), 2010 International Conference on*, 2010, pp. V8-248-V8-252.

[33] J. López Vizcaíno, Y. Ye, and I. Tafur Monroy, "Energy efficiency analysis for flexible-grid OFDM-based optical networks," *Computer Networks,* vol. 56, pp. 2400-2419, 7/5/ 2012.

[34] M. Klinkowski and K. Walkowiak, "Offline RSA algorithms for elastic optical networks with dedicated path protection consideration," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on*, 2012, pp. 670-676.

[35] H. Saini and A. K. Garg, "Protection and Restoration Schemes in Optical Networks: A Comprehensive Survey," *International Journal,* vol. 2, 2013.

[36] J.-P. Vasseur, M. Pickavet, and P. Demeester, *Network recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*: Elsevier, 2004.

[37] S. Yuan and J. P. Jue, "Shared protection routing algorithm for optical network," *Optical Networks Magazine,* vol. 3, pp. 32-39, 2002.

[38] SLA INFORMATION ZONE, "Service Level Agreement Zone", 2015. [Online]. Disponível em: http://www.sla-zone.co.uk/. [Acesso em: 09- Jan- 2016].

[39] O. Aboul-Magd and S. Rabie, "RFC 4115 - A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic", *IETF Tools*, 2005. [Online]. Disponível em: https://tools.ietf.org/html/rfc4115. [Acesso em: 10- Jan- 2016].

[40] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numerische mathematik,* vol. 1, pp. 269-271, 1959.

[41] P. Feofiloff, "Algoritmo de Dijkstra", *Algoritmos para grafos*, 2015. [Online]. Disponível em: http://www.ime.usp.br/~pf/algoritmos_para_grafos/aulas/dijkstra.html. [Acesso em: 10- Jan- 2016].

[42] A. S. Tanenbaum, *Sistemas operacionais modernos*, 3 ed.: Prentice-Hall do Brasil, 2010.

[43] M. P. dos Santos, "Introdução à simulação discreta," *Rio de Janeiro: UERJ,* 1999.

[44] J. Sztrik, "Basic queueing theory," *University of Debrecen: Faculty of Informatics,* 2011.

[45] S. Qiao and L. Qiao, "A robust and efficient algorithm for evaluating Erlang B formula," *Canada: McMaster University,* 1998.

[46] M. Rausand and A. Høyland, *System Reliability Theory: Models, Statistical Methods, and Applications*, 2 ed.: Wiley, 2004.

APÊNDICE A – PSEUDOCÓDIGO DO ALGORITO DE *DIJKSTRA*

```
<variáveis globais>
N: INTEIRO;

ALGORITMO "Dijkstra"

<parâmetros de entrada>
custo[0..N-1, 0..N-1], fonte, destino: INTEIRO;

<variáveis locais>
DECLARE v,u: INTEIRO;
DECLARE Q: FILA<INTEIRO>;
DECLARE parent[0..N-1], distancia[0..N-1]: INTEIRO;

INICIO

PARA v ← 0 ATÉ N-1 FAÇA
        SE (custo[fonte,v] ≠ INFINITO) ENTÃO
                distancia[v] ← custo[fonte, v];
                parent[v]  ← fonte;
                INSERE_NA_FILA(Q,v);
        SENÃO
                parent[v] ← -1;
                distancia[v] ← INFINITO;
        FIM-SE
FIM-PARA
ENQUANTO ( Q ≠ VAZIO ) FAÇA
        u ← EXTRAIR_MIN(Q);
        SE (distancia[u] = INFINITO) ENTÃO
                INTERROMPA;
        SE (distancia[v] > distancia[u] + custo[u, v]) ENTÃO
                distancia[v] ← distancia[u] + custo[u, v];
                parent[v] ← proximo;
                INSERE_NA_FILA(Q,v);
        FIM SE
FIM-ENQUANTO

<backtraking>

DECLARE rota:FILA<INTEIRO>;
DECLARE dist: INTEIRO;

INSERE_PRIMEIRO_NA_FILA(rota,d);
v ← parent[d];

ENQUANTO (v ≠ fonte E v ≠ -1) FAÇA
        INSERE_PRIMEIRO_NA_FILA(rota,v);
        v ← parent[v];
FIM-ENQUANTO

SE (v = fonte) ENTÃO
        INSERE_PRIMEIRO_NA_FILA(rota,fonte);
SENÃO
        rota ← VAZIO;
FIM-SE
dist ← distancia[destino];
RETORNA [rota, dist];
FIM

FIM-ALGORITMO
```

APÊNDICE B – PSEUDOCÓDIGO DO ALGORITO *FIRST-FIT*

```
REGISTRO FSU
        pos: INTEIRO;
        status: ENUM{IDLE,USED,SHARED};
        pruned: BOOLEANO;
        shared_count : INTEIRO;
FIM-REGISTRO

<variáveis globais>
N: INTEIRO;
NFSU: INTEIRO;

ALGORITMO "Fist-fit"

<parâmetro de entrada>
rota: FILA<INTEIRO>;
banda_requerida: INTEIRO;
permite_compartilhar: BOOLEANO;
banda[0..N-1, 0..N-1, 0...NFSU-1]: FSU;
best_effort: BOOLEANO;

<variáveis locais>
DECLARE i, j, w, x, y, z: INTEIRO;
DECLARE base, fs: INTEIRO;
DECLARE fit: BOOLEANO;

INICIO
fit ← False;
PARA fs ←banda_requerida ATÉ 1 FAÇA
        k ← 0;
        base ← 0;
        ENQUANTO ( k < LEN(rota)-1 E fit ≠ True) FAÇA
                i ← rota[k];
                j ← rota[k+1];
                w ← 0;
                PARA z ← base ATÉ NFSU-1 FAÇA
                        SE (permite_compartilhar) ENTÃO
                                SE (banda[i][j][z].status = IDLE E banda[i][j][z].pruned ≠ True) ENTÃO
                                        w ← w+1;
                                SENÃO
                                        base ← z+1;
                                        k ← -1;
                                        INTERROMPE;
                                FIM-SE
                        SENÃO
                                SE (banda[i][j][z].status ≠ USED E banda[i][j][z].pruned ≠ True) ENTÃO
                                        w ← w+1;
                                SENÃO
                                        base ← z+1;
                                        k ← -1;
                                        INTERROMPE;
                                FIM-SE
                        FIM-SE
                        SE (w = fs) ENTÃO
                                SE (k = LEN(rota)-1) ENTÃO
                                        fit ← True;
                                FIM-SE
                                INTERROMPE;
                        FIM-SE
                FIM-PARA
                k ← k+1;
        FIM-ENQUANTO
        SE ( fit = True OU best_effort ≠ True) ENTÃO
                INTERROMPE;
        FIM-SE
```

```
FIM-PARA
SE ( fit = True) ENTÃO
        RETORNA [base,fs];
SENÃO
        RETORNA NÃO_ENCONTRADO;
FIM-PARA
FIM

FIM-ALGORITMO

ALGORITMO "Fist-fit Inverso"

<parâmetro de entrada>
banda_requerida: INTEIRO;
rota: FILA<INTEIRO>;
permite_compartilhar: BOOLEANO;
banda[0..N-1, 0..N-1, 0...NFSU-1]: FSU;

<variáveis locais>
DECLARE i, j, w, x, y, z: INTEIRO;
DECLARE base, fs: INTEIRO;
DECLARE fit: BOOLEANO;

INICIO
fit ← False;
w ←NFSU-1;
z ← w;
ENQUANTO ( fit ≠ True ) FAÇA
        SE (w < fs-1) ENTÃO
                INTERROMPE;
        FIM-SE
        SE (z = -1) ENTÃO
                INTERROMPE;
        FIM-SE
        z ← z-1;
        PARA k ← 0 ATÉ k < LEN(rota)-1 FAÇA
                i ← rota[k];
                j ← rota[k+1];
                SE (permite_compartilhar) ENTÃO
                        SE (banda[i][j][z+1].status = USED OU banda[i][j][z+1].pruned ) ENTÃO
                                w ← z;
                                INTERROMPE;
                        FIM-SE
                SENÃO
                        SE (banda[i][j][z+1].status ≠ IDLE OU banda[i][j][z+1].pruned ) ENTÃO
                                w ← z;
                                INTERROMPE;;
                        FIM-SE
                FIM-SE
                SE (w-z = fs E k = LEN(rota)-1) ENTÃO
                        fit ← True;
                        INTERROMPE;
                FIM-SE
        FIM-PARA
FIM-ENQUANTO
SE ( fit = True) ENTÃO
        base ← w-fs+1;
        RETORNA [base,fs];
SENÃO
        RETORNA NÃO_ENCONTRADO;
FIM-PARA
FIM

FIM-ALGORITMO
```

APÊNDICE C – PSEUDOCÓDIGO DO ALGORITMO CAMINHO DE TRABALHO

```
REGISTRO FSU
        pos: INTEIRO;
        status: ENUM{IDLE,USED,SHARED};
        pruned: BOOLEANO;
        shared_count : INTEIRO;
FIM-REGISTRO

<variáveis globais>
N: INTEIRO;
NFSU: INTEIRO;
custo[1..N, 1..N]: INTEIRO;
banda[0..N-1, 0..N-1, 0...NFSU-1]: FSU;

ALGORITMO "Caminho de Trabalho"

<parâmetro de entrada>
fonte, destino: INTEIRO;
banda_requerida: INTEIRO;
best_effort : BOOLEANO;

<variáveis locais>
DECLARE custo_temp[1..N, 1..N];
DECLARE i, j, k: INTEIRO;
DECLARE rota: FILA<INTEIRO>;
DECLARE permite_compartilhar : BOOLEANO;

INICIO
        permite_compartilhar ←False;
        COPIA custo EM custo_temp;
        APLICA HEURÍSTICAS (custo_temp); <Opcional./Caso exista>
        rota = Dijkstra(fonte,destino,custo_temp);
        SE (rota ≠ NULO) ENTÃO
                [base,fs] = First-fit(rota,banda_requerida, permite_compartilhar ←False, banda, best_effort);
                SE ([base,fs] ≠ NULO) ENTÃO
                        RETORNA [rota, base,fs];
                SENÃO
                        RETORNA NULO;
                FIM-SE
        SENÃO
                RETORNA NULO;
        FIM-SE
FIM

FIM-ALGORITMO
```

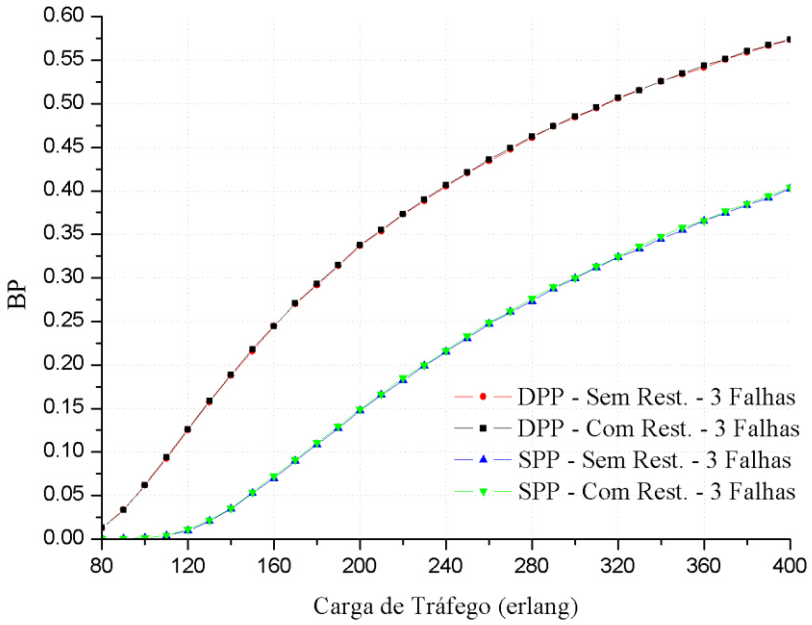
APÊNDICE D – PSEUDOCÓDIGO DO ALGORITMO *DPP*

```
REGISTRO FSU
        pos: INTEIRO;
        status: ENUM{IDLE,USED,SHARED};
        pruned: BOOLEANO;
        shared_count : INTEIRO;
FIM-REGISTRO

<variáveis globais>
N: INTEIRO;
NFSU: INTEIRO;
custo[1..N, 1..N]: INTEIRO;
banda[0..N-1, 0..N-1, 0...NFSU-1]: FSU;

ALGORITMO "DPP"

<parâmetro de entrada>
fonte, destino: INTEIRO;
banda_requerida: INTEIRO;
caminho_trabalho: LISTA<INTEIRO>;

<variáveis locais>
DECLARE custo_temp[1..N, 1..N];
DECLARE i, j, k: INTEIRO;
DECLARE rota: FILA<INTEIRO>;

INICIO
        COPIA custo EM custo_temp;
        PARA k ← 0 ATÉ k < LEN(caminho_trabalho)-1 FAÇA
                i ← caminho_trabalho[k];
                j ← caminho_trabalho[k+1];
                custo_temp[i][j] = INFINITO;
        FIM-PARA
        rota = Dijkstra(fonte,destino,custo_temp);
        SE (rota ≠ NULO) ENTÃO
                [base,fs] = First-fit(rota,banda_requerida, permite_compartilhar ←False, banda, best_effort ←False);
                SE ([base,fs] ≠ NULO) ENTÃO
                        RETORNA [rota, base,fs];
                SENÃO
                        RETORNA NULO;
                FIM-SE
        SENÃO
                RETORNA NULO;
        FIM-SE
FIM

FIM-ALGORITMO
```

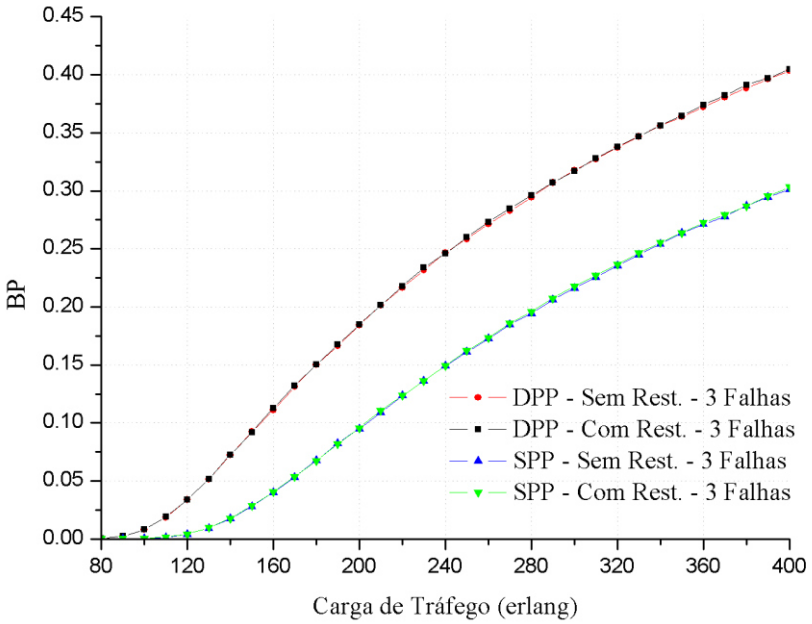
APÊNDICE E – PSEUDOCÓDIGO DO ALGORITMO *SPP*

```
REGISTRO FSU
        pos: INTEIRO;
        status: ENUM{IDLE,USED,SHARED};
        pruned: BOOLEANO;
        shared_count : INTEIRO;
FIM-REGISTRO

<variáveis globais>
N: INTEIRO;
NFSU: INTEIRO;
custo[0..N-1, 0..N-1]: REAL;
banda[0..N-1, 0..N-1, 0...NFSU-1]: FSU;

ALGORITMO "SPP"

<parâmetro de entrada>
fonte, destino: INTEIRO;
banda_requerida: INTEIRO;
caminho_trabalho: LISTA<INTEIRO>;

<variáveis locais>
DECLARE custo_temp[1..N, 1..N] : REAL;
DECLARE banda_temp[0..N-1, 0..N-1, 0...NFSU-1]: FSU;
DECLARE i, j, k: INTEIRO;
DECLARE rota: FILA<INTEIRO>;
DECLARE permite_compartilhar , best_effort : BOOLEANO;

INICIO
        best_effort ← False;
        permite_compartilhar ←True;
        COPIA custo EM custo_temp;
        COPIA banda EM banda_temp;
        APLICA HEURÍSTICAS (custo_temp); <Opcional./Caso exista>
        <Podar todas subportadoras do link utilizada pelo caminho primário atual, ou seja, anule o enlace>
        PARA k ← 0 ATÉ k < LEN(caminho_trabalho)-1 FAÇA
                i ← caminho_trabalho[k];
                j ← caminho_trabalho[k+1];
                custo_temp[i][j] = INFINITO;
        FIM-PARA
        <Podar as subportadoras dos caminhos de backup cujos caminhos primários transpassam o caminho primário atual>
        PARA CADA espectro_z pertencente aos enlaces_{i,j} da rota dos caminho de backup cujos caminhos primários
        intersectam o caminho_trabalho FAÇA
                banda_temp [i][j][z].pruned ← True;
        FIM-PARA
        rota = Dijkstra(fonte,destino,custo_temp);
        SE (rota ≠ NULO) ENTÃO
                SE POSSUI_HEURISTICA_IDS ENTÃO
                        [base,fs] = first-fit_inverso(rota,banda_requerida, permite_compartilhar, banda_temp);
                SENÃO
                        [base,fs] = first-fit(rota,banda_requerida, permite_compartilhar, banda_temp, best_effort);
                FIM-SE
                SE ([base,fs] ≠ NULO) ENTÃO
                        RETORNA [rota, base,fs];
                SENÃO
                        RETORNA NULO;
                FIM-SE
        SENÃO
                RETORNA NULO;
        FIM-SE

FIM

FIM-ALGORITMO
```

APÊNDICE F – GRÁFICO BP DO EXPERIMENTO G1 PARA 3 FALHAS



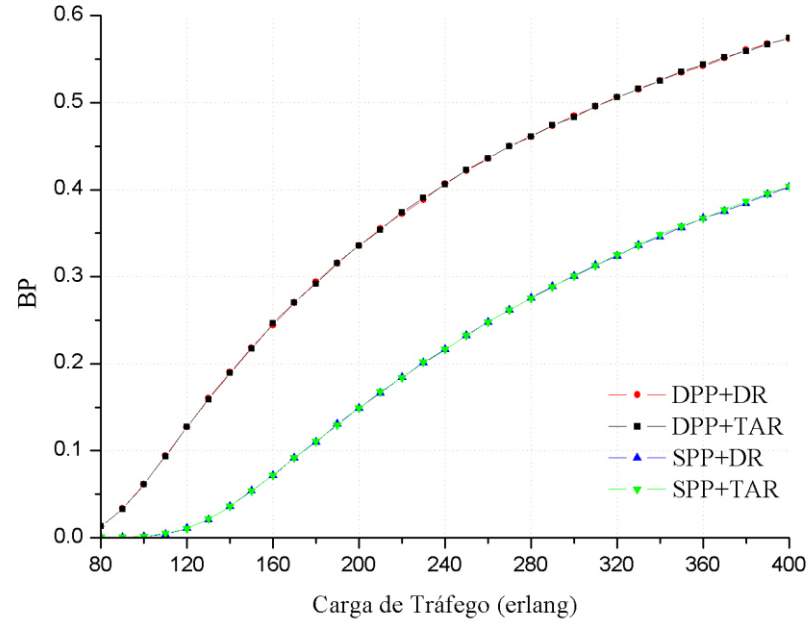
a)



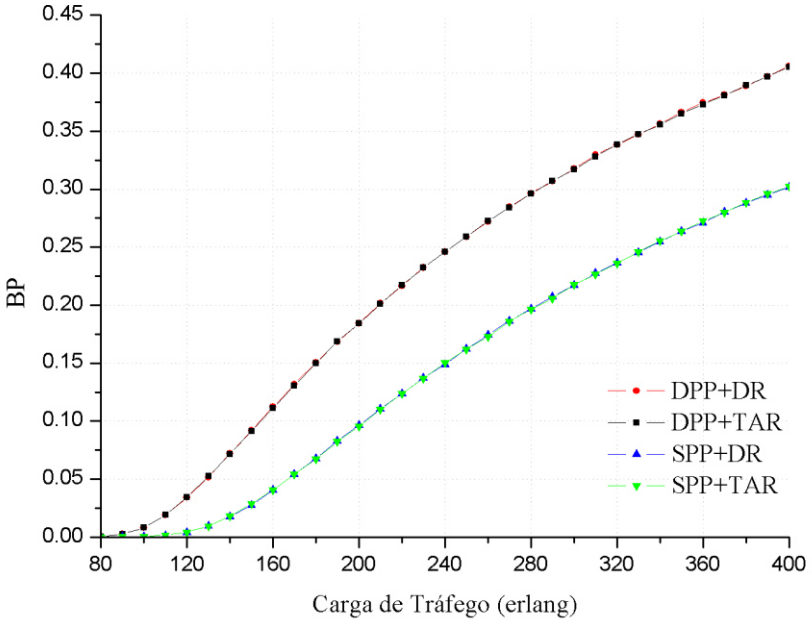
b)

Figura 80 - Gráfico de BP comparando DPP x SPP com e sem restauração para 3 falhas simultâneas: a) NSFNET; b) USNET.

APÊNDICE G – GRÁFICOS BP, SUR E AHOP DO EXPERIMENTO G2

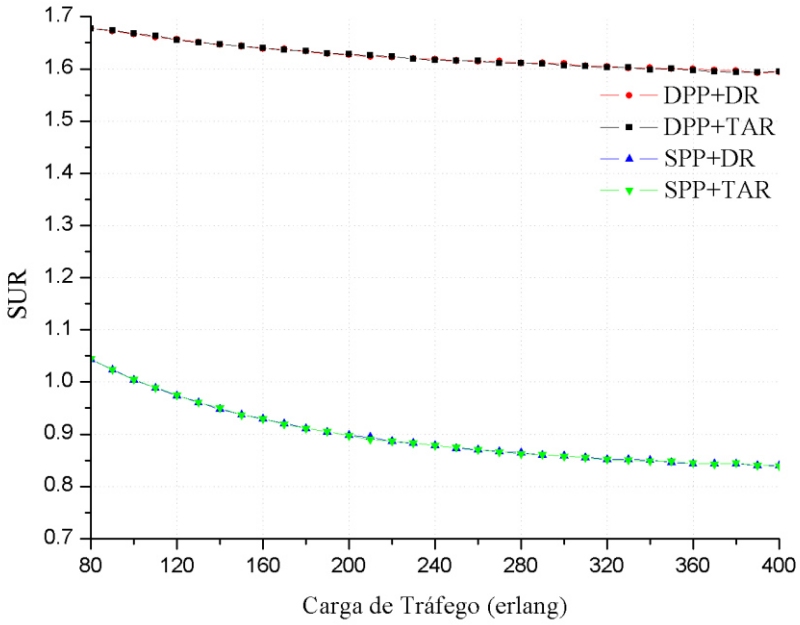


a)

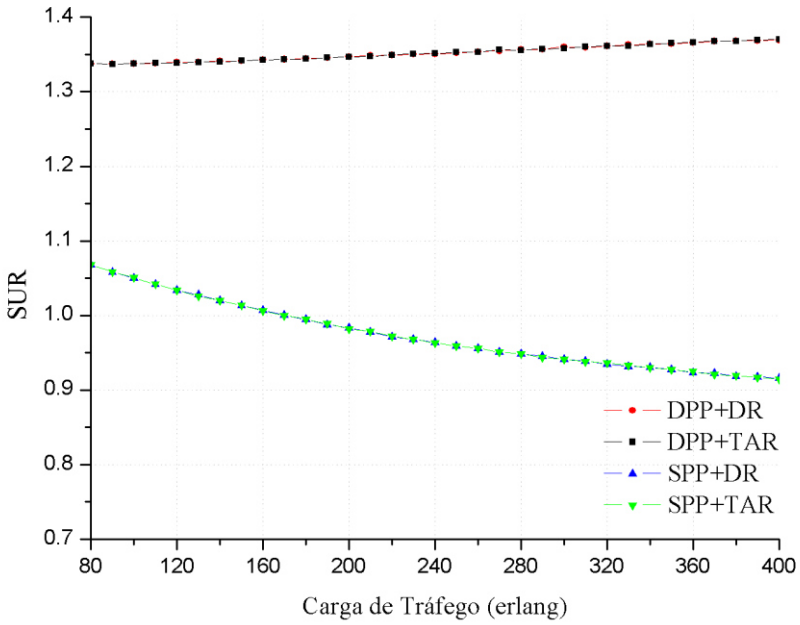


b)

Figura 81 - Gráfico de BP comparando DR x TAR: a) NSFNET; b) USNET.

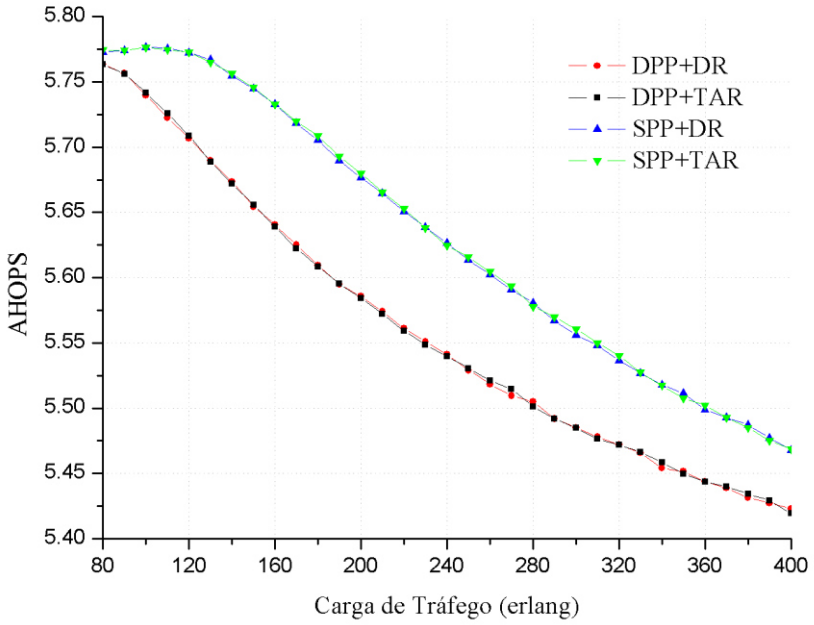


a)

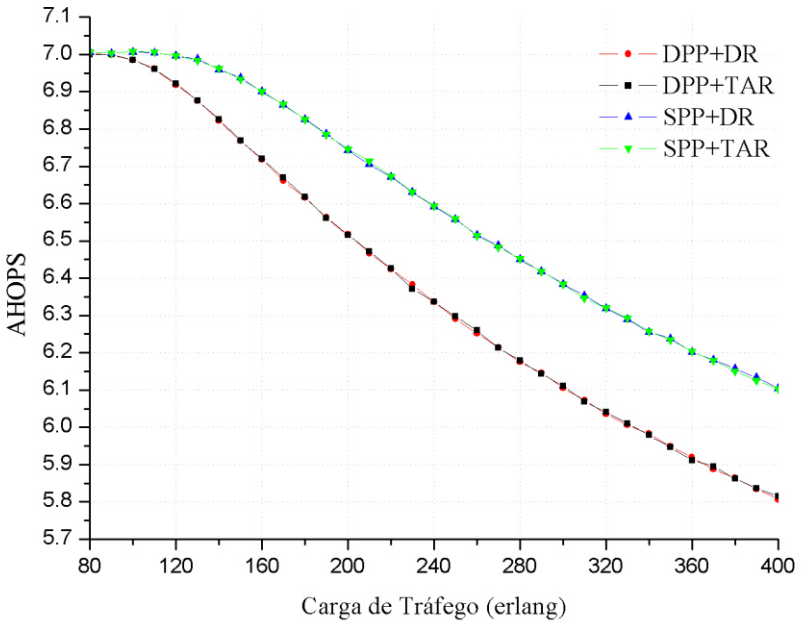


b)

Figura 82 - Gráfico de SUR comparando DR x TAR: a) NSFNET; b) USNET.



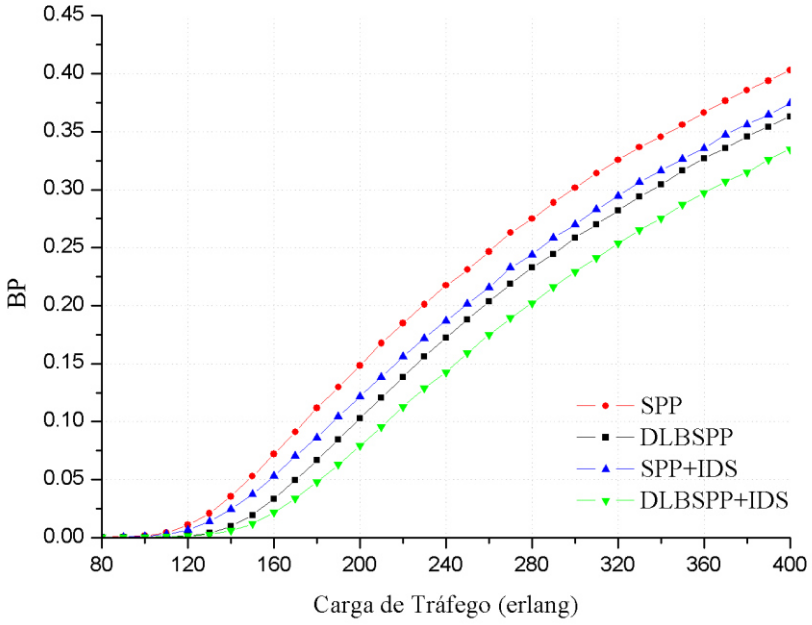
a)



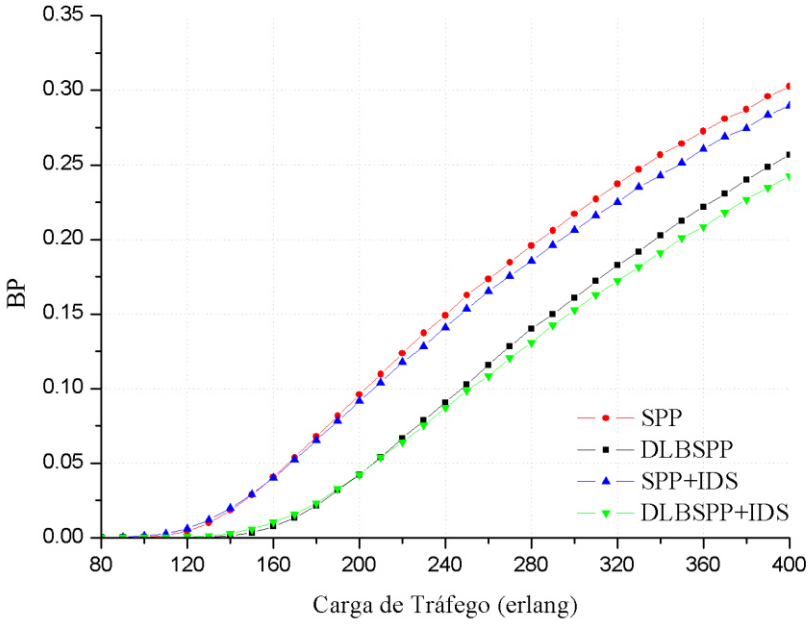
b)

Figura 83 - Gráfico de AHOP comparando DR x TAR: a) NSFNET; b) USNET.

APÊNDICE H – GRÁFICOS BP, SUR E AHOP DO EXPERIMENTO G5

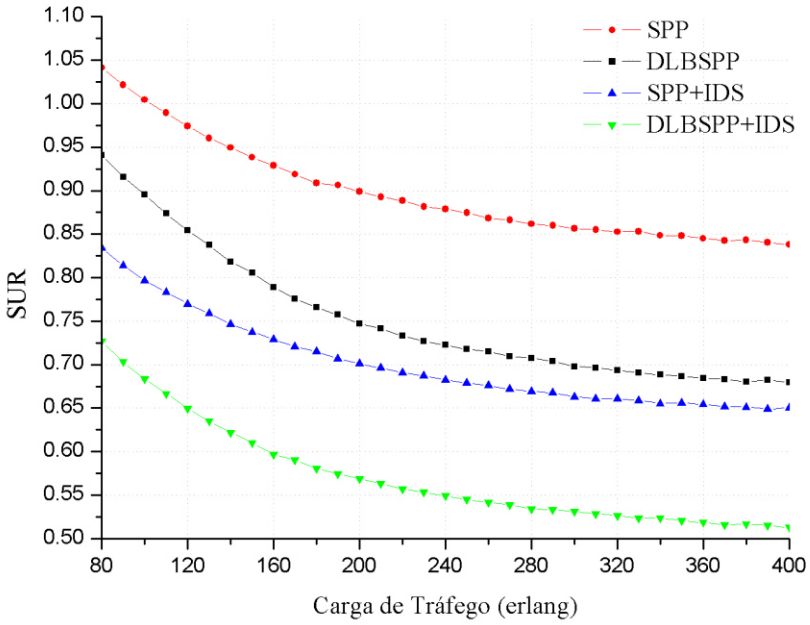


a)

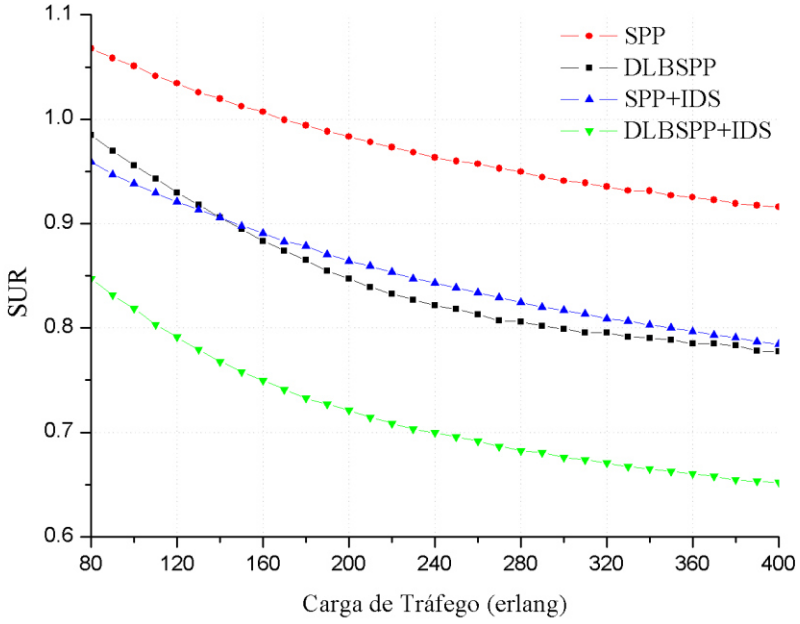


b)

Figura 84 - Gráfico de BP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET.

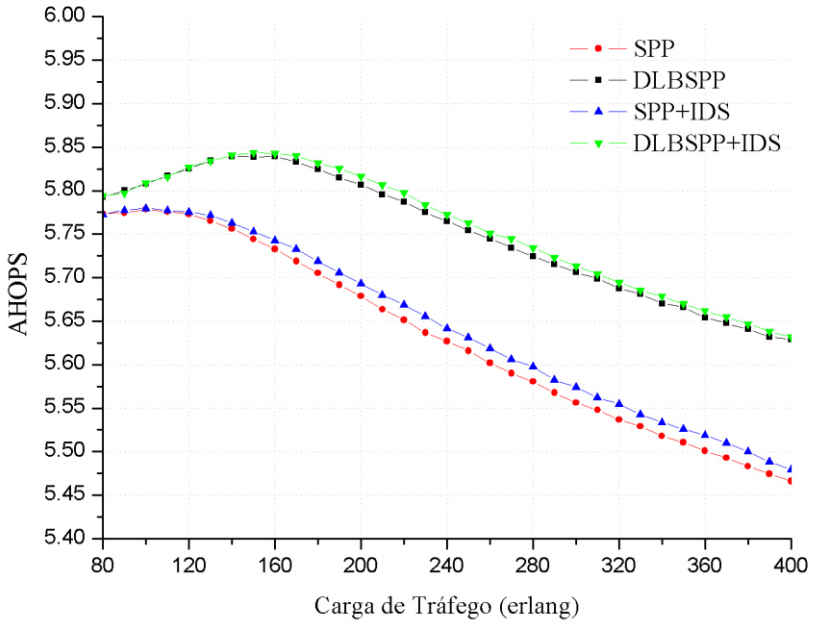


a)

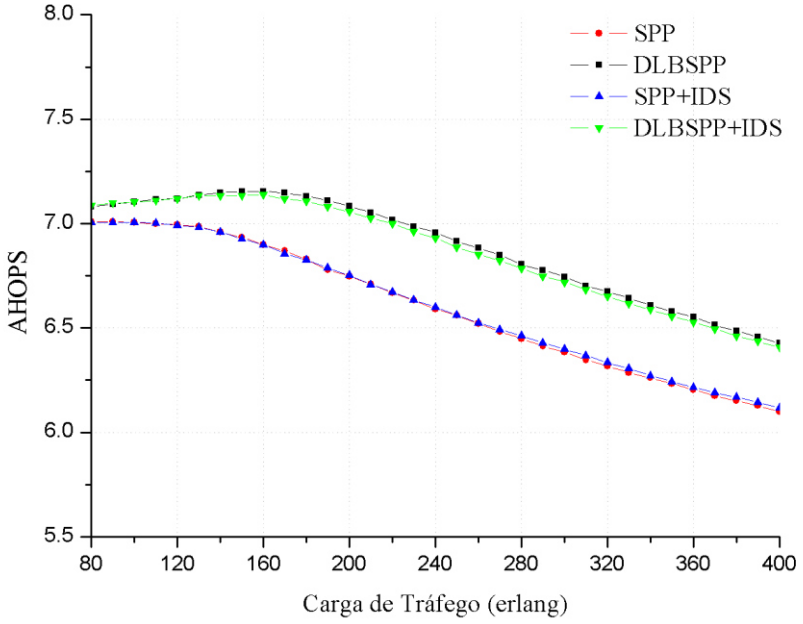


b)

Figura 85 - Gráfico de SUR comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET.



a)



b)

Figura 86 - Gráfico de AHOP comparando SPP, DLBSPP, SPP IDS, DLBSPP IDS com restauração dinâmica: a) NSFNET; b) USNET.