Restauração dirigida por conexões de baixa prioridade e recursos de *backup* em cenários de desastres em *EON*

Tatiana de O. Silva[1], Rodrigo A. Costa[1], Helder M. N. S. Oliveira[3], Juliana de Santi[2], Gustavo B. Figueiredo[1]

[1]Departamento de Ciência da Computação – Universidade Federal da Bahia (UFBA)

[2]Universidade Tecnológica Federal do Paraná (UTFPR) – Curitiba

[3]Universidade Federal do Pará (UFPA) - Belém

silva.tati.do@gmail.com, alencarcosta3@gmail.com, heldermay@ufpa.br,

jsanti@utfpr.edu.br, gustavobf@ufba.br

Abstract. *Elastic Optical Networks (EON) have shown to be a solution for the future of optical transport networks. However, failure events can cause vigorous data loss. For this, protection and restoration schemes have been developed in order to minimize such damage, such as this work that proposes a survivability scheme with bandwidth degradation and delay in restoration to low-priority connections transmitted in the backup path of high priority connections. Comparations with the dedicated backup path protection strategy demonstrate superiority in our algorithm, noteworthy that the degradation policy favors reducing the blocking probability.*

Resumo. *As Redes Ópticas Elásticas (Elastic Optical Networks - EON) tem se mostrado uma solução para o futuro das redes de transporte óptico. No entanto, eventos de falhas podem causar a perda vigorosa de dados. Para isso esquemas de proteção e restauração tem sido desenvolvidos a fim de minimizar tal prejuízo, a exemplo deste trabalho que propõe um esquema de sobrevivência com degradação de banda e atraso na restauração para conexões de baixa prioridade transmitidas no caminho de backup de conexões de alta prioridade. Comparações com a estratégia de proteção de caminho com backup dedicado demonstram superioridade em nosso algoritmo salientando que a política de degradação favorece redução da probabilidade de bloqueio.*

1. Introdução

A grande quantidade de dispositivos e usuários, bem como a demanda para uma diversidade de aplicações e serviços tem elevado as exigências em relação à qualidade de serviço e a taxa de transmissão na Internet [Cisco 2018]. Neste contexto, as Redes Ópticas Elásticas (*EON - Elastic Optical Network*) apresentam-se como uma solução promissora para suprir estas demandas de forma eficiente. Através da multiplexação por divisão de frequência ortogonal *(OFDM – Orthogonal Frequency Division Multiplexing)*, as redes *EONs*, separam os recursos espectrais em sub portadoras, alocando o tamanho do espectro de forma proporcional ao volume de tráfego requisitado garantindo, assim, eficiência e escalabilidade. Além disso, estas redes apresentam eficiência energética e permitem

ajustes entre a necessidade dos recursos da rede e o formato de modulação com diferentes alcances e diferentes taxas de transmissão de dados [Wang et al. 2012].

Embora as EONs garantam alta disponibilidade e eficiência no uso de recursos, não se pode ignorar a iminência de perda massiva de dados ocasionada por desastres naturais (furacões, terremotos, etc.), acidentes e ataques maliciosos, dentre outros, os quais podem afetar a infraestrutura óptica com múltiplas falhas em enlaces e equipamentos. Tais problemas podem levar à perda permanente de dados e interrupção de serviços com diferentes níveis de criticidade. Desta forma, as estratégias de proteção e/ou restauração são fundamentais para a recuperação de desastres. As duas abordagens são consideradas complementares, sendo a proteção um esquema proativo e a restauração, um esquema reativo que provêm a utilização eficiente dos recursos ópticos disponíveis para garantir a sobrevivência da rede .

Mecanismos de proteção [Júnior and Drummond 2017, Anoh et al. 2017, Assis et al. 2019] possuem um plano pré-definido com recursos redundantes reservados/alocados para prover a recuperação de falhas, enquanto que a restauração [Shen et al. 2016, Regis et al. 2018, Ferdousi et al. 2020, Halder et al. 2020, da Silva Oliveira and Fonseca 2019] estabelece este plano considerando os recursos disponíveis após o evento da falha. Ao mesmo tempo em que garantem 100% de recuperação, as estratégias de proteção apresentam custo elevado uma vez que os recursos de *backup* são utilizados somente se a falha ocorrer, essa por sua vez, é imprevisível. Por outro lado, ao não realizar reserva antecipada, as estratégias de restauração apresentam maior eficiência na utilização dos recursos disponíveis ao custo de não prover garantia total de recuperação. Assim, na restauração a proporção de garantia de recuperação de conexões interrompidas dependente da eficiência na adaptação dos recursos usados tanto pelas conexões interrompidas quanto pelas conexões não afetadas pelas falhas.

Mediante escassez de recursos, o provisionamento de recursos para as conexões pode ser adaptado de acordo com a tolerância à degradação de serviço [Regis et al. 2018, Santos et al. 2018] especificada pelos requisitos de *QoS (Quality of Service)* em contratos de serviço *SLA (Service Level Agreement)* com o provedor dos serviços [Agrawal et al. 2017, Khan et al. 2021, Saxena and Goel 2021]. Além disso, estas especificações estão relacionadas a classes de serviço, as quais organizam as conexões em classes com diferentes prioridades e seus respectivos níveis de tolerância à degradação de serviço (por exemplo, degradação de banda passante, tolerância para atraso na restauração, etc.). Classes de maior prioridade apresentam maiores restrições à degradação de serviço, enquanto classes de menor prioridade são mais flexíveis à degradação. Desta forma, a classificação das conexões e suas respectivas especificações de *SLA* devem ser levadas em consideração na definição de estratégias de recuperação de desastres a fim de identificar as melhores oportunidades para aumentar a capacidade de provisionamento ou reprovisionamento da rede.

Este artigo propõe uma estratégia híbrida que aborda técnicas de proteção e restauração, através do algoritmo denominado *Path Protection and Restoration based on Bandwidth Degradation and Restoration Delay (PPRD)*, para o problema de recuperação de múltiplas falhas causadas por desastres. O algoritmo *PPRD* faz uso das classes de serviço de alta e baixa prioridade e usufrui da proteção 1:1 com tráfego extra transmitindo

conexões de alta prioridade no caminho principal, enquanto o tráfego de baixa prioridade é estabelecido no caminho *backup* das conexões de alta prioridade durante a transmissão normal da rede. Na ocorrência de falhas não há qualquer processo de sinalização adicional para estabelecer um caminho *backup* para as conexões de alta prioridade, sendo o tráfego do caminho principal comutado para o caminho *backup* previamente reservado. Além disso, o algoritmo emprega os mecanismos de degradação de banda e tempo para as conexões de baixa prioridade que foram afetadas pelo desastre e para as novas conexões de baixa prioridade que continuarem chegando na rede durante a falha.

Os resultados mostram que a restauração baseada na degradação de serviços e na utilização de recursos de *backup* reduz a probabilidade de bloqueio geral da rede e a probabilidade de bloqueio por classes. Além disso, a estratégia proposta aumenta a capacidade de restauração de conexões de baixa prioridade interrompidas pelo desastre enquanto mantém a capacidade de restauração de conexões de alta prioridade.

As demais seções deste artigo estão organizadas da seguinte forma. A Seção 2 discute alguns trabalhos relacionados ao problema de recuperação de desastres. A Seção 3 introduz o algoritmo proposto para a recuperação de desastres baseado em degradação de serviço e utilização de recursos de *backup*. A Seção 4 apresenta um estudo de avaliação de desempenho do algoritmo proposto e a Seção 5 destaca as conclusões.

2. Trabalhos Relacionados

O estudo sobre reprovisionamento torna-se fundamental em *EON* devido à imensa quantidade de informações que trafegam nas redes diariamente. À medida que a quantidade de dados cresce, aumenta também a preocupação em desenvolver novas técnicas de proteção e restauração eficientes. E assim, problemas de interrupção de serviços com diferentes níveis de criticidade, por conta de falhas, devem ser minimizados o máximo possível.

Em [Ferdousi et al. 2020], os autores propõem heurística de recuperação de serviços após um evento de desastre mediante duas estratégias: alocação de recursos seletiva e adaptativa. Por considerar a recuperação total e parcial de elementos de rede com base nos recursos disponíveis em cada estágio, a recuperação da nuvem no pós-desastre produz uma rápida recuperação de serviços e alocação eficiente de recursos. Assim, nosso trabalho também compatibiliza mecanismos de sobrevivência mediante evento de desastre, agregando alocação prévia de recursos a fim de aumentar a recuperação da rede.

No trabalho de [Santos and Figueiredo 2020] a técnica *hybrid Multi-Attribute Decision Making* é utilizada para realizar preempção de *lihtpaths* em Redes Ópticas Elásticas. A diferenciação dos *lihtpaths* é feita de três maneiras: através da preservação dos recursos da rede para caminhos de luz de alta prioridade, do uso de diferentes algoritmos de roteamento e fazendo preempção e rerroteamento de caminhos de luz de baixa prioridade para aceitar os de alta prioridade. Apresentamos uma técnica híbrida com diferenciação de serviços, privilegiando a classe de alta prioridade e fazendo rerroteamento da classe de baixa prioridade, acrescida de flexibilização de banda e tempo.

Em [Stapleton 2019], uma arquitetura de proteção é introduzida e são empregados os conceitos de agrupamento de portadoras ópticas de sinalização e classes de serviços para realizar proteção mista. Desta forma, incorpora a proteção selecionada que visa reduzir os recursos reservados ao tráfego de alta prioridade e a proteção compartilhada que

oferece flexibilidade dos recursos de proteção para vários caminhos. Através das abordagens hierárquicas *Network Media Channels* e *Media Channels* verificou-se a redução na necessidade de banda-guarda entre canais. Apesar de considerar a utilização de proteção e conexões com diferentes prioridades os autores não levam em consideração a restauração.

Em [Regis et al. 2018], são apresentados os algoritmos *Differentiated Restoration based Multipath* e *DiffRM-Nao-Gradual*. Os autores consideram quatro diferentes classes de serviços e introduzem o conceito de degradação máxima de banda passante e atraso de restauração. As contribuições consistem no aumento do número de conexões restauradas, além da redução da probabilidade de bloqueio. Apesar de considerar a utilização de restauração e conexões com diferentes prioridades de tráfego os autores não levam em consideração técnicas de proteção, as quais são creditadas em nossa abordagem para as classes de serviço de alta e baixa prioridade.

Os autores em [Lisboa et al. 2018] propõem o algoritmo *Restoration of Differentiated Cloud Services based on Bandwidth Degradation and Restoration Delay*. O trabalho aborda o serviço de restauração em nuvem óptica e os resultados mostram melhorias significativas na fase de restauração mediante tolerância ao atraso e redução da banda para três classes específicas de serviço. Comparativamente, levamos em consideração técnicas de proteção e avaliamos a probabilidade de bloqueio por classe de serviço.

O algoritmo proposto *PPRD* se diferencia dos trabalhos mencionados por compatibilizar a técnica de sobrevivência híbrida de proteção dedicada com tráfego extra (*DPP - Data Path Protection*) [Papadimitriou and Mannie 2006], para conexões de baixa prioridade que aproveitam os recursos de backup para serem transmitidas, e a recuperação de serviços após um evento de desastre. Neste cenário são consideradas diferentes classes de serviços e esquemas de degradação de banda e tempo para classes de baixa prioridade, possibilitando a elas maior taxa de recuperação, reduzindo assim a chance de se perderem durante sua transferência na rede. Tal abordagem demonstra melhor utilização dos recursos e, portanto maior provisionamento.

3. O Algoritmo PPRD

O algoritmo *Path Protection and Restoration based on Bandwidth Degradation and Restoration Delay* (**PPRD**) é um algoritmo híbrido que faz uso de um mecanismo de proteção dedicada 1:1, onde conexões de baixa prioridade são provisionadas em caminhos ópticos de *backup* de conexões de alta prioridade, e um mecanismo de restauração com diferenciação de serviço. Desta forma, é possível reduzir a subutilização de recursos e aumentar o número de conexões atendidas durante a fase de provisionamento, e aumentar a capacidade de restauração durante o processo de recuperação de desastres. São estudadas duas classes de serviço (alta prioridade (*AP*) e baixa prioridade (*BP*)), para as quais são considerados níveis de degradação de banda e tolerância ao atraso na restauração de acordo com as especificações de contrato de serviço SLA de cada classe (Seção 3.2).

O algoritmo proposto utiliza um grafo auxiliar G para representar os recursos ópticos disponíveis durante a operação normal de rede e durante a recuperação de desastres. Para cada par origem-destino, são consideradas as $K = 3$ menores rotas disjuntas, as quais são usadas no estabelecimento de caminhos principais e de caminhos de *backup*. As seções a seguir apresentam o modelo para estabelecimento das conexões solicitadas (Seção 3.1), as características das classes de serviço usadas (Seção 3.2) e a descrição e

complexidade do algoritmo proposto (Seções 3.3 - 3.4).

3.1. Estabelecimento das conexões solicitadas

O algoritmo *PPRD* ocorre em duas etapas formalizadas pelo Algoritmo 1 (provisionamento) e pelo Algoritmo 2 (restauração). Na fase de provisionamento, as requisições para estabelecimento de conexão, que chegam na rede de forma dinâmica, são representadas pela tupla $R(O, D, B, P)$, com seus componentes definindo o par de nós origem-destino O-D de R, demandando B unidades de banda passante e com prioridade P. O conceito de classes e prioridades (Seção 3.2) é usado para det erminar em quais caminhos (principal e/ou caminho *backup*) as conexões devem ser provisionadas. A classe de alta prioridade utiliza exclusivamente o caminho principal enquanto a classe de prioridade baixa só dispõe de caminhos de *backup* reservados para as conexões de alta prioridade. A política de alocação de *slots* é a *First-Fit*. O estabelecimento de uma nova conexão é realizado em uma das *K* menores rotas com recursos disponíveis. Quando ocorre um desastre, a fase de recuperação/restauração é ativada levando-se em consideração o estado atual dos recursos ópticos disponíveis na rede e o conjunto de conexões interrompidas pelo desastre. Nesta fase, o conceito de classes e prioridades (Seção 3.2) é levado em consideração para determinar a liberação de recursos de *backup*, em qual caminho cada conexão deve ser restaurada e quais conexões podem sofrer degradação de serviço (degradação de banda e atraso na restauração) de forma a viabilizar sua restauração mediante restrição de recursos.

3.2. Prioridade, classes de serviço e degradação

No cenário considerado neste trabalho, as conexões são classificadas em Classes de Serviço (*Class of Services - CoS*) de acordo com sua tolerância para degradação de banda e tolerância ao atraso de restauração. Conforme apresentado na Tabela 1, as conexões que chegam na rede são rotuladas como Alta Prioridade *(AP)* e Baixa Prioridade *(BP)*, e obedecem aos requisitos de *QoS* relacionados ao tipo de prioridade e a degradação permitida de acordo com o contrato de *SLA* [Assis et al. 2019]. Neste trabalho, o provisionamento é feito para garantir a recuperação máxima das conexões de alta prioridade, assim, aloca-se o caminho principal e o caminho *backup* para estas conexões. Para aproveitar os recursos ociosos, as conexões de baixa prioridade são provisionadas nos caminhos de *backup*.

Tabela 1. Classes de serviços, prioridade e degradação de serviço.

Classe de Serviço	Prioridade	Degradação (%)	Atraso de Restauração
Alta Prioridade (AP)	alta	0%	não permitido
Baixa Prioridade (BP)	baixa	50/70%*	permitido

*Conexões de baixa prioridade afetadas pelo desastre são degradadas em 50%. Novas conexões de baixa prioridade que chegam durante a fase de recuperação da rede são degradadas em 70%.

Logo que as falhas são identificadas, a rede tenta sobreviver utilizando os recursos que sobraram. As conexões que foram afetadas pelo desastre são separadas por classe: para as de alta prioridade, a transmissão do caminho principal é alterada para seu caminho *backup*; as de baixa prioridade buscam por caminhos *backup* de conexões de alta prioridade que não foram afetados e que estejam disponíveis para a tentativa de restauração. Assim que liberam o caminho *backup* da alta prioridade, as conexões de baixa prioridade

afetadas têm sua banda degradada em 50%, para então realizar sua primeira tentativa de restauração. Ou seja, verifica o quanto de banda a conexão já havia transmitido antes do desastre e quanto falta para concluir a transmissão e, em seguida calcula o número de *slots* necessários para transmitir apenas metade da banda que falta transmitir. Caso não haja recursos suficientes para transferir a conexão, ela será postergada e futuramente faz outra tentativa de restauração, se não conseguir será bloqueada. Simultaneamente ao processo de recuperação, a rede continua a receber novas conexões, tanto de alta prioridade, quanto de baixa prioridade. Para as novas conexões de alta prioridade, o processo de provisionamento não é alterado. Por outro lado, para as conexões de baixa prioridade a tentativa de provisionamento é realizada considerando uma degradação de 70% da banda passante originalmente requisitada. Assim, verifica qual a banda demandada para a conexão e calcula o número de *slots* para transmitir apenas 0.7 da banda desta conexão. Para as conexões de baixa prioridade, o tempo é postergado como forma de compensar a degradação da banda passante.

3.3. Operação do algoritmo

O funcionamento do Algoritmo *PPRD* é composto pelas etapas de provisionamento (Algoritmo 1) e restauração (Algoritmo 2), levando-se em consideração os requisitos, parâmetros e modelo de estabelecimento das conexões descritos na Seção 3.1. O algoritmo proposto é uma adaptação do algoritmo *Data Path Protection (DPP)* [Papadimitriou and Mannie 2006] acrescido: 1) do mecanismo de utilização de caminho de *backup* para o provisionamento de conexões de baixa prioridade; 2) do mecanismo de recuperação de desastres baseado em restauração diferenciada. No algoritmo *DPP*, um caminho de proteção dedicado protege exatamente um caminho principal e, em condições sem falhas, o tráfego é transmitido apenas no caminho principal, deixando o caminho de *backup* reservado para ser utilizado futuramente se houver falha.

O algoritmo PPRD - Provisionamento (Algoritmo 1) é executado toda vez que uma nova conexão R chega na rede, ou quando é chamado pelo Algoritmo 2 na tentativa de reprovisionar uma conexão interrompida pelo desastre (podendo ser uma tentativa imediatamente após o desastre ou uma tentativa de restauração postergada). Em ambos os casos, a requisição de conexão *R*, com prioridade P, chega dinamicamente solicitando provisionamento entre o par origem *O* e destino *D*. Novas requisições de conexão chegam na rede independentemente se a rede opera em modo $NORMAL$ ou em modo $DESASTRE$, ou seja, durante a fase de recuperação das falhas ocasionadas pelo desastre. Assim, dependendo do modo de operação da rede, o Algoritmo 1 pode usar degradação de serviço no provisionamento de classes de baixa prioridade.

Como o algoritmo PPRD considera diferenciação de serviço, o primeiro passo para o provisionamento é verificar qual a prioridade de requisição. Se R é de alta prioridade (Linha 1), busca-se um caminho principal CP com o número de *slots* necessários para atender a requisição de B unidades de banda passante (Linha 2) e, caso exista CP, busca-se um caminho de *backup* CB para R (Linha 6) com os mesmos requisitos de CP. A busca por CP e CB leva em consideração as $K = 3$ menores rotas entre O-D. Caso haja recursos disponíveis para alocar CP e CB, a requisição de conexão R é provisionada no caminho principal CP (Linha 12). Caso contrário, R é bloqueada (Linhas 9-10). É importante notar que, como as conexões de alta prioridade não são tolerantes à degradação de serviço, a forma como é realizado seu provisionamento é independente do modo de

operação (NORMAL ou DESASTRE) da rede.

Algoritmo 1: PPRD - Provisionamento

Entrada : Requisição $R(O, D, B, P)$ entre os nós (O-D), demandando B unidades de banda passante, com prioridade P. Grafo $G(V, E)$ representando a rede. $MODO$ que determina se a rede opera ou não em situação de DESASTRE.
Saída : Caminho principal/*backup* entre (O-D)

1 **Se** $P(R) == AP$ **Então**
  `// R é de alta prioridade`
2 $CP \leftarrow$ RMLSA $(G, slots(B), O, D)$;
3 $G \leftarrow G/E(CP)$;
4 $CP[R] \leftarrow CP$;
5 **Se** $\exists\, CP$ **Então**
6 $CB \leftarrow$ RMLSA $(G, slots(B), O, D)$;
7 $G \leftarrow G/E(CB)$;
8 $CB[R] \leftarrow CB$;
9 **Se** $\nexists\, CP$ *ou* $\nexists\, CB$ **Então**
10 Bloqueia R;
11 **Senão**
12 Provisiona R em CP;
13 **Senão**
  `// R é de baixa prioridade`
14 **Se** $MODO == DESASTRE$ **Então**
15 **Se** $Tentativas\_de\_restauração[R] == 0$ **Então**
  `// R é uma nova conexão`
16 $B \leftarrow Degrada\_Req(B, 0.7)$;
17 $lpBackup \leftarrow Extrai\_Caminho\_MAX\_Slots(CB[O][D])$;
18 **Se** $(slots(B(lpBackup)) \geq B)$ *e* $(duração(R) \leq duração(lpBackup))$ **Então**
19 Provisiona/restaura R em $lpBackup$;
20 $Req\_BP[R] \leftarrow lpBackup$;
21 **Senão se** $Tentativas\_de\_restauração[R] == 1$ **Então**
22 $CI \leftarrow R$;
23 **Senão**
24 Bloqueia/Descarta R;
25 onde:AP é alta prioridade; $CP[R]$ conjunto principal de R; $CB[R]$ caminho *backup* de R; $Req\_BP[R]$ caminho de *backup* usado pela conexão R de baixa prioridade; $CB[O][D]$ conjunto de caminhos *backup* entre O-D; $lpBackup$ um *lightpath backup* extraído do conjunto $CB[O][D]$; CI conjunto das conexões interrompidas pelo desastre.

A partir da Linha 13, o Algoritmo 1 considera o provisionamento de conexões de baixa prioridade. Caso a rede esteja operando em modo de DESASTRE (Linha 14) e R seja uma nova requisição de conexão, ou seja, esta conexão não sofreu nenhuma tentativa de restauração (Linha 15), a banda passante B originalmente demandada é degradada em 70% (Linha 16). Como há escassez de recursos em decorrência do desastre, a ideia é usar a flexibilidade de degradação de serviço provida pelas conexões de baixa prioridade de forma a atender R com uma banda menor do que a banda originalmente requisitada ao invés de bloqueá-la. Adicionalmente, esta estratégia não estrangula ainda mais os recursos já escassos, dando oportunidade para que outras conexões sejam aceitas e/ou restauradas. Por outro lado, se R não é uma nova conexão, ou seja, é uma conexão

que foi interrompida pelo desastre (Algoritmo 2) e está na sua tentativa de recuperação, então R já teve sua banda degradada em 50% (na Linha 7 do Algoritmo 2) e precisa ser reprovisionada (o Algoritmo 2 chama o Algoritmo 1 para reprovisionar as conexões de baixa prioridade interrompidas pelo desastre). Entre as Linhas 17-24 o funcionamento do Algoritmo 1 é o mesmo para novas requisições de conexão e para conexões que estão tentando ser reprovisionadas. Na Linha 17, busca-se, no conjunto de caminhos *backup* do par origem-destino O-D ($CB[O][D]$), o caminho $lpBackup$ de *backup* com a maior quantidade de *slots* disponíveis. Se a quantidade de *slots* de $lpBackup$ é suficiente para provisionar/reprovisionar R e a duração de R é menor ou igual à duração de $lpBackup$ (Linha 18), então a conexão é provisionada em $lpBackup$ e $lpBackup$ é armazenado no conjunto de caminho de *backup* em utilização por conexões de baixa prioridade (Linha 20). Se não é possível encontrar $lpBackup$ capaz de atender R, e R é uma conexão na sua tentativa de restauração imediatamente até o desastre, então R é adicionada ao conjunto de conexões interrompidas pelo desastre (CI) para uma tentativa de restauração postergada (Linhas 12-14 do Algoritmo 2). Caso, R seja uma nova conexão ou uma conexão que já usou sua tentativa de restauração postergada, então R é bloqueada/descartada (Linha 24).

Após um evento de desastre, o mecanismo de restauração do PPRD (Algoritmo 2) é executado. Neste contexto, considera-se o conjunto CI de conexões interrompidas devido ao desastre e o estado da rede (grafo G') após o desastre. No algoritmo PPRD - Restauração, as conexões são restauradas levando-se em consideração as prioridades e os requisitos descritos na Tabela 1. O conjunto CI é uma fila ordenada por prioridade, ou seja, são consideradas primeiro todas as conexões de alta prioridade e depois todas as conexões de baixa prioridade, não havendo ordem específica entre conexões de mesma prioridade.

A restauração de conexões de alta prioridade interrompidas pelo desastre é feita de forma direta para seus respectivos caminhos de *backup*. Assim, o primeiro passo para a restauração de cada conexão c de alta prioridade (Linha 2) no conjunto CI é retirar as conexões de baixa prioridade que foram provisionadas (Algoritmo 1) no caminho de *backup* $CB[c]$ de c (Linhas 3-4). Para tal, as conexões de baixa prioridade retiradas do caminho $CB[c]$ são armazenado no conjunto CI (Linha 4) para posterior tentativa de reprovisionamento. Com o caminho de *backup* livre, c é restaurada em $CB[c]$ (Linha 5), ou seja, o recurso reservado para a proteção de c foi usado.

Após o desastre a disponibilidade de recursos é drasticamente reduzida e, desta forma, a ideia do algoritmo PPRD - Restauração é usar a tolerância para degradação de serviço provida pelas conexões pertencentes à classe de baixa prioridade (Tabela 1) para aumentar as chances de restauração de um maior número de conexões. A primeira tentativa de restauração para cada conexão de baixa prioridade em CI é feita imediatamente após o desastre (Linhas 7-11). Neste caso, a banda passante B originalmente demandada é degradada em 50% (Linha 8) e a duração de c é atualizada (Linha 9) levando-se em consideração a quantidade de dados já transmitidos antes do desastre. Para fins de controle do algoritmo PPRD, o número de tentativas de restauração é incrementado (Linha 10). Então, o Algoritmo 1 é chamado (Linha 11) com a banda já degradada e especificando-se a classe de c (BP) e modo DESASTRE. Caso os recursos ópticos sejam insuficientes para restaurar c imediatamente após o desastre (Linhas 21 - 22 no Algoritmo 1), então a tolerância ao atraso na restauração (Tabela 1) é empregada, e uma

Algoritmo 2: PPRD - Restauração

Entrada : Conjunto CI das conexões interrompidas pelo desastre. Grafo $G'(V, E)$ com o estado da rede após o desastre.
Saída : Conexão c restaurada, descartada ou reagendada para nova tentativa de restauração com degradação de serviço.

```
1  Para c ∈ CI Faça
2      Se p(c) == AP Então
3          Enquanto ∃ CB[c] Faça
4              CI ← CB[c];
5          Restaura c em CB[c]
6      Senão
           // Conexão de baixa prioridade
7          Se Tentativas_de_restauração[c] == 0 Então
               // Tentativa de restauração imediatamente após
                  desastre
8              B ← Degrada_Req(B, 0.5);
9              Atualiza_duração(c);
10             Tentativas_de_restauração[c] + +;
11             Algoritmo 1(c, BP, G', DESASTRE);
12         Senão se Tentativas_de_restauração[c] == 1 Então
               // Restauração postergada
13             Tentativas_de_restauração[c] + +;
14             Agenda_Execução(Algoritmo 1(c, BP, G', DESASTRE));
15         Senão
16             Descarta c;
17 onde: AP é alta prioridade; BP é baixa prioridade; CB[c] caminho backup de c.
```

nova tentativa de restauração é agendada, ou seja, a restauração é postergada, e executada através de chamada para o Algoritmo 1 (Linhas 12 - 14). Neste caso, a degradação de banda e atualização de duração de c já foram ajustadas na tentativa de restauração realizada imediatamente após o desastre (Linhas 8 - 9). Se mesmo após a tentativa de restauração postergada, não for possível reprovisionar a conexão devido à indisponibilidade de recursos, então c é descartada (Linha 16).

3.4. Complexidade do Algoritmo

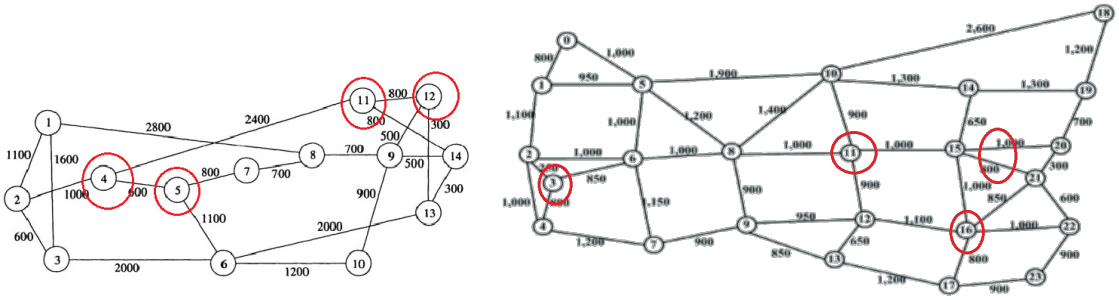
Na etapa de provisionamento (Algoritmo 1), o cálculo dos caminhos mais curtos entre um par de nós (Linhas 2 e 6) é feito pelo algoritmo de *Dijkstra* $O(n^2)$. Na etapa de restauração, são realizadas até c chamadas (Linha 1) para o Algoritmo 1 (Linhas 11 e 14), onde c é uma constante. Assim, a complexidade do algoritmo *PPRD* é O(n^2).

4. Avaliação de desempenho

A fim de avaliar a eficácia do algoritmo *PPRD*, foram executadas simulações usando um simulador *ad-hoc* de eventos discretos desenvolvido na linguagem *Python* através da biblioteca *SimPy*. Foi usado o método da replicação para 20 amostras com diferentes sementes e em cada execução foram geradas 100.000 requisições distribuídas uniformemente entre todos os pares origem e destino. O processo de chegada das conexões segue a distribuição de *Poisson* e todas elas obedecem uma distribuição exponencial negativa

com média de 60 unidades de tempo [Savas et al. 2014]. A classificação em CoS segue a distribuição uniforme (50% alta prioridade e 50% baixa prioridade).

A degradação de banda é realizada mediante a ocorrência do desastre: 50% para conexões de baixa prioridade e que foram interrompidas pelo desastre [Lisboa et al. 2018]; e 70% para novas requisições de conexão de baixa prioridade. Este nível se mostrou o mais adequado após testes exaustivos utilizando outros percentuais de degradação conforme os resultados apresentados. A fim de compensar a degradação da banda das conexões de baixa prioridade, elas podem ser atrasadas uma única vez caso não sejam imediatamente restauradas. As simulações foram feitas utilizando a topologia NSF (Figura 1(a)), com 14 nós e 19 enlaces, e a topologia *USA* (Figura 1(b)), com 24 nós e 43 enlaces bidirecionais.



(a) NSF [Lisboa et al. 2018] (b) USA [Bao et al. 2016]

Figura 1. Topologias de rede utilizadas.

As falhas [Rausand and Hoyland 2003, Sztrik et al. 2012] simuladas neste trabalho correspondem às áreas de desastre que estão destacadas nas Fig. 1(a) segundo [Lisboa et al. 2018] e Fig. 1(b) segundo [Bao et al. 2016, Regis et al. 2018]. Elas são distribuídas de modo uniforme através de todos os enlaces da fibra e o intervalo entre uma falha e outra possui valores médios respectivamente de 1000 e 10 unidades de tempo. Todas as falhas ocorrem de forma sequencial e as zonas atingidas ficam interrompidas pelo desastre até que haja reparo, o qual ocorre proporcionalmente ao tempo de recuperação de todos os nós e enlaces da rede.

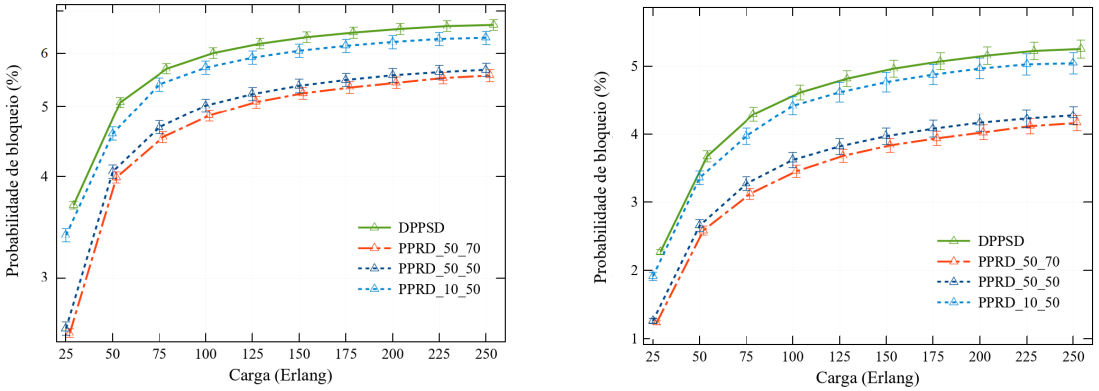
As requisições geradas possuem as seguintes larguras de banda uniformemente distribuídas: 10Gbps, 20Gbps, 40Gbps, 80Gbps e 100Gbps. O espectro de enlace foi dividido em 300 *slots* de subportadoras, com 12.5GHz de frequência cada. Diferentes formatos de modulação e taxas de bits são considerados baseando-se na distância entre os nós da rede: BPSK, QPSK, 8QAM e 16QAM. A política de alocação de espectro utilizada foi a *First-Fit*.

As seguintes métricas foram utilizadas: probabilidade de bloqueio *(PB)*, definida pela razão entre a quantidade de requisições bloqueadas e o total de requisições, a probabilidade de bloqueio por classe e o número de conexões restauradas por classe. O nível de confiança reportado nos resultados é de 95%.

São apresentadas quatro curvas nos gráficos: DPPSD, que representa o algoritmo DPP Sem Degradação de serviço; PPRD_50_**70**, que descreve os resultados para o algoritmo proposto PPRD que permite 50% de degradação de banda das conexões interrompidas e 70% das novas conexões mediante desastre; PPRD_50_**50** que descreve os resultados

para o algoritmo proposto PPRD que permite 50% de degradação de banda das conexões interrompidas e 50% das novas conexões mediante desastre; PPRD_10_**50** que descreve os resultados para o algoritmo proposto PPRD que permite 10% de degradação de banda das conexões interrompidas e 50% das novas conexões mediante desastre . Estas duas últimas curvas são apresentada para que se possa visualizar o ajuste de parâmetros.

A Fig. 2 apresenta a probabilidade de bloqueio (PB). Para a topologia NSF (Fig. 2(a)), os valores de PB produzidos pelo algoritmo PPRD são menores do que os valores gerados pelo algoritmo DPPSD. Diferentemente do DPPSD, a operação do algoritmo proposto PPRD permite: 1) a utilização de recursos de *backup* das conexões de alta prioridade para transferir dados de conexões de baixa prioridade; 2) e a degradação da banda de novas conexões de baixa prioridade de forma a adaptá-las à situações de escassez de recursos devido ao desastre. Assim, aumenta-se as chances de aceitação de requisições de baixa prioridade sem desconsiderar a proteção das conexões de alta prioridade. Levando-se em consideração diferentes ajustes de degradação de banda para as novas conexões, o PPRD_50_70 gera valores de PB menores do que os valores de PB gerados por PPRD_50_50 e o PPRD_10_50. Esta diferença se mantém nos demais resultados gerados e, assim, serão apresentados no gráfico para verificação, mas sem descrição específica. Para a topologia USA (Fig. 3(b)), o comportamento das curvas é o mesmo da topologia NSF, mas com valores de PB menores em consequência da maior conectividade da topologia USA.

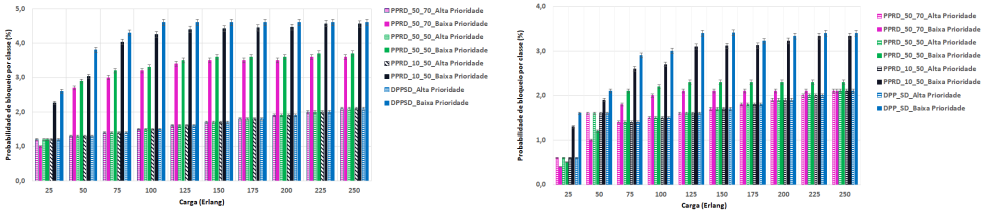


(a) NSF (b) USA

Figura 2. Probabilidade de bloqueio.

A probabilidade bloqueio por classes de serviço é apresentada na Fig. 3. Para ambas as topologias NSF (Fig. 3(a)) e USA (Fig. 3(b)), os algoritmos comparados geram, para a maioria das cargas, a mesma probabilidade de bloqueio para a classe de alta prioridade, mostrando que a utilização do caminho de *backup* das conexões de alta prioridade para provisionar conexões de baixa prioridade, bem como o emprego de restauração não impactam a capacidade do PPRD em provisionar conexões de alta prioridade e sua respectiva proteção (*backup*). O DPPSD opta somente pelo provisionamento de conexões de alta prioridade e seus caminhos de proteção exclusivos. Por outro lado, através de seu mecanismo alternativo de provisionamento, o PPRD bloqueia, para carga de 250 *Erlangs*, no máximo 3.6% e 2.1% das conexões de baixa prioridade para NSF e USA, respectivamente. Isso mostra que o algoritmo proposto explora melhor os recursos disponíveis,

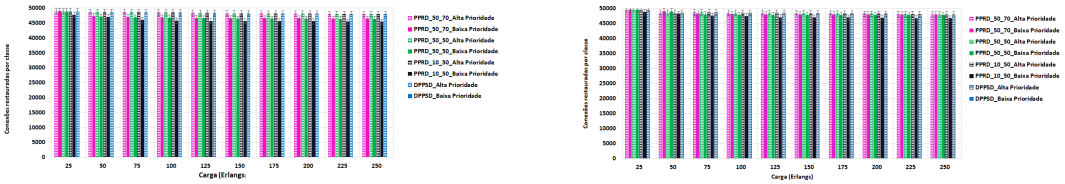
sendo vantajoso tanto para o cliente, com mair aceitação de conexões, quanto para o provedor de serviços, que pode administrar melhor suas demandas de forma a aumentar sua receita ao reduzir o bloqueio de conexões.



(a) NSF (b) USA

Figura 3. Probabilidade de bloqueio por classes.

O número de conexões restauradas para cada classe de serviço é apresentado na Fig. 4. Como há uso de proteção 1:1 (com caminhos disjuntos) em todos os algoritmos comparados, todas as conexões de alta prioridade que foram interrompidas pelo desastre foram recuperadas. Para a topologia NSF (Fig. 4(a)), com carga de 250 *Erlangs*, o PPRD_50_70 restaura aproximadamente 48780 conexões de baixa prioridade que foram interrompidas pelo desastre. Por outro lado, o DPPSD restaura apenas as conexões de alta prioridade através de proteção 1:1 [Papadimitriou and Mannie 2006]. A capacidade de restauração do PPRD está diretamente ligada à três fatores: 1) o uso de caminhos de *backup* de conexões de alta prioridade (não afetadas pelo desastre) para a restauração de conexões de baixa prioridade; 2) a tolerância à degradação de banda das conexões de baixa prioridade interrompidas pelo desastre; e 3) a tolerância ao atraso na restauração destas conexões mediante a indisponibilidade de recursos para recuperação imediata. Isso mostra a capacidade do algoritmo PPRD em adaptar a operação da rede de acordo com a disponibilidade de recursos ópticos existentes. Para a topologia USA (Fig. 4(b)), o mecanismo de restauração diferenciada do algoritmo PPRD também mostra maior eficiência do que a abordagem DPPSD em relação ao número de conexões restauradas.



(a) NSF (b) USA

Figura 4. Conexões restauradas.

5. Conclusão e Trabalhos Futuros

Devido ao alto volume de tráfego transmitido nas redes ópticas, o uso de esquemas de sobrevivência eficientes é de fundamental importância. Este artigo apresentou um algoritmo híbrido para sobrevivência em redes EON que faz uso de proteção para requisições de alta prioridade aliado ao compartilhamento de caminho *backup* para conexões de baixa prioridade. Além disso, o algoritmo proposto lança mão de duas técnicas importantes para

aumentar a utilização da rede, minimizando a probabilidade de bloqueio. A primeira técnica é a degradação de banda das requisições de baixa prioridade enquanto a rede esta sob escassez de recursos devido à ocorrência de falhas. A segunda técnica é a postergação da restauração das conexões de baixa prioridade que não podem ser reprovisionadas imediatamente após o desastre devido à indisponibilidade de recursos. Resultados obtidos via simulação mostraram que o algoritmo proposto é capaz de reduzir a probabilidade de bloqueio e preservar a relação de prioridade entre as classes. Adicionalmente, fica evidente que o uso do algoritmo proposto é capaz de aumentar a capacidade de restauração das requisições afetadas por desastres.

Como trabalhos futuros, propõe-se a investigação do impacto de diferentes níveis de degradação de serviço para a classe de baixa prioridade. A adoção de níveis diferenciados de modulação para as classes de alta e baixa prioridade é outra hipótese de pesquisa que deverá ser investigada em trabalhos futuros.

Referências

Agrawal, A., Vyas, U., Bhatia, V., and Prakash, S. (2017). SLA-aware differentiated QoS in elastic optical networks. *Optical Fiber Technology*, 36:41–50.

Anoh, N. G., Babri, M., Kora, A. D., Faye, R. M., Aka, B., and Lishou, C. (2017). An efficient hybrid protection scheme with shared/dedicated backup paths on elastic optical networks. *Digital Communications and Networks*, 3(1):11–18.

Assis, K. D., Almeida, R., Waldman, H., Santos, A., Alencar, M., Reed, M., Hammad, A., and Simeonidou, D. (2019). SLA formulation for squeezed protection in elastic optical networks considering the modulation format. *IEEE/OSA Journal of Optical Communications and Networking*, 11(5):202–212.

Bao, N.-H., Tornatore, M., Martel, C. U., and Mukherjee, B. (2016). Fairness-aware degradation based multipath re-provisioning strategy for post-disaster telecom mesh networks. *Journal of Optical Communications and Networking*, 8(6):441–450.

Cisco, F. (2018). Cisco Visual Networking Index (VNI). Complete Forecast Update, 2017-2022. `https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/knowledge-network-webinars/pdfs/1213-business-services-ckn.pdf`. Último acesso: 14/04/2021.

da Silva Oliveira, H. M. N. and Fonseca, N. (2019). Proteção em redes ópticas elásticas com multiplexação espacial. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 161–168. SBC.

Ferdousi, S., Tornatore, M., Dikbiyik, F., Martel, C. U., Xu, S., Hirota, Y., Awaji, Y., and Mukherjee, B. (2020). Joint progressive network and datacenter recovery after large-scale disasters. *IEEE Transactions on Network and Service Management*, 17(3):1501–1514.

Halder, J., Acharya, T., Chatterjee, M., and Bhattacharya, U. (2020). On spectrum and energy efficient survivable multipath routing in off-line elastic optical network. *Computer Communications*, 160:375–387.

Júnior, P. J. and Drummond, A. C. (2017). Proteçao por pré-provisionamento em redes opticas elásticas. In *Workshop em Desempenho de Sistemas Computacionais e de Comunicação (WPerformance)*. SBC.

Khan, S., Hussain, F. K., and Hussain, O. K. (2021). Guaranteeing end-to-end QoS provisioning in SOA based SDN architecture: A survey and open issues. *Future Generation Computer Systems*, 119:176–187.

Lisboa, F., Fonseca, K. V., and de Santi, J. (2018). Restauração de serviços em nuvem óptica: uma abordagem tolerante à degradação de banda e ao atraso de restauração. *Revista Eletrônica de Iniciação Científica em Computação*, 16(3).

Papadimitriou, D. and Mannie, E. (2006). Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS). RFC 4427.

Rausand, M. and Hoyland, A. (2003). *System reliability theory: models, statistical methods, and applications*, volume 396. John Wiley & Sons.

Regis, G. B., Fonseca, K. V., Figueiredo, G. B., and de Santi, J. (2018). Adoção de restauração com degradação diferenciada em redes EONs para a recuperação de desastres. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*. SBC.

Santos, A. S., de Santi, J., and Figueiredo, G. B. (2018). Uma estratégia online para degradação de serviço com qos proporcional em redes Ó pticas elásticas. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, Porto Alegre, RS, Brasil. SBC.

Santos, A. S. and Figueiredo, G. B. (2020). Uma abordagem de decisão multi-critério para preempção de caminhos de luz em eon. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 239–252. SBC.

Savas, S. S., Habib, M. F., Tornatore, M., Dikbiyik, F., and Mukherjee, B. (2014). Network adaptability to disaster disruptions by exploiting degraded-service tolerance. *IEEE Communications Magazine*, 52(12):58–65.

Saxena, J. and Goel, A. (2021). Differentiated services and its importance in fault tolerant WDM optical network. *Optical and Quantum Electronics*, 53(3):1–17.

Shen, G., Guo, H., and Bose, S. K. (2016). Survivable elastic optical networks: survey and perspective. *Photonic Network Communications*, 31(1):71–87.

Stapleton, M. (2019). *Protection and Restoration Schemes in Elastic Optical Networks*. PhD thesis, Université d'Ottawa/University of Ottawa.

Sztrik, J. et al. (2012). Basic queueing theory. *University of Debrecen, Faculty of Informatics*, 193:60–67.

Wang, Y., Cao, X., Hu, Q., and Pan, Y. (2012). Towards elastic and fine-granular bandwidth allocation in spectrum-sliced optical networks. *IEEE/OSA Journal of Optical Communications and Networking*, 4(11):906–917.