UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
CAMPUS CHAPECÓ
CURSO DE CIÊNCIA DA COMPUTAÇÃO

ANÁLISE DO IMPACTO DE TÉCNICAS DE SOBREVIVÊNCIA EM REDES ÓPTICAS ELÁSTICAS DE TELECOMUNICAÇÕES

ARISTIDES DARLAN PEITER TONDOLO

CHAPECÓ
2018

ARISTIDES DARLAN PEITER TONDOLO

ANÁLISE DO IMPACTO DE TÉCNICAS DE SOBREVIVÊNCIA EM REDES ÓPTICAS ELÁSTICAS DE TELECOMUNICAÇÕES

Trabalho de conclusão de curso de graduação apresentado como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.
Orientador: Prof. Dr. Claunir Pavan

CHAPECÓ
2018

Tondolo, Aristides Darlan Peiter

Análise do Impacto de Técnicas de Sobrevivência em Redes Ópticas Elásticas de Telecomunicações / por Aristides Darlan Peiter Tondolo. – 2018.
50 f.: il.; 30 cm.

Orientador: Claunir Pavan
Monografia (Graduação) - Universidade Federal da Fronteira Sul, Ciência da Computação, Curso de Ciência da Computação, RS, 2018.

1. Redes ópticas elásticas. 2. Bloqueio em redes ópticas. 3. Sobrevivência em redes ópticas. 4. RMLSA. I. Pavan, Claunir. II. Título.

E-mail: adpeiter@hotmail.com

ARISTIDES DARLAN PEITER TONDOLO

ANÁLISE DO IMPACTO DE TÉCNICAS DE SOBREVIVÊNCIA EM REDES ÓPTICAS ELÁSTICAS DE TELECOMUNICAÇÕES

Trabalho de conclusão de curso de graduação apresentado como requisito para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.

Orientador: Prof. Dr. Claunir Pavan

Aprovado em: 05\07\2018

BANCA EXAMINADORA:

Dr. Claunir Pavan - UFFS

Dr. Marco Aurélio Spohn - UFFS

Dr. Bráulio Adriano de Melo - UFFS

AGRADECIMENTOS

Ao professor e orientador, Dr. Claunir Pavan.

Ao professor Dr. Marco Aurélio Spohn.

Ao professor Dr. Braulio Adriano de Melo.

A estes três docentes, em especial, agradeço por todos os momentos de ensinamento, inclusive aqueles além do assunto da matéria que estavam ministrando.

Ao orientador, em particular, pelo auxílio, paciência e confiança no trabalho.

RESUMO

Nas redes ópticas de telecomunicações, o bloqueio é um evento de não estabelecimento de uma conexão requisitada e é frequentemente utilizado como parâmetro de avaliação do desempenho da rede. Quanto menor o bloqueio, mais a rede está capacitada a suportar a demanda de tráfego que recebe.

Uma característica presente nas redes atuais é a sobrevivência, que possibilita conexão entre quaisquer nós da rede, mesmo quando há uma situação de falha. No entanto, a sobrevivência necessita de uma quantidade considerável de recursos para ser provida e isto pode impactar na ocorrência de eventos de bloqueio.

Tornar uma rede sobrevivente impõe várias tarefas que interferem na sua performance, no custo e também na complexidade do seu controle. Nas eminentes redes óticas elásticas, o problema de rotear e alocar o tráfego da rede evoluiu para um problema ainda mais complexo que nas redes fixas tradicionais. Nestas últimas, devem estar satisfeitas as restrições de continuidade e contiguidade, cuja severidade é maior que nas anteriores.

Considerando que estas novas características podem ocasionar efeitos diferenciados no funcionamento da rede, o objetivo deste estudo foi avaliar a relação entre estratégias de proteção e outras propriedades afetadas por estas estratégias. Comparamos as taxas de bloqueio e de utilização de recursos para proteção dedicada e compartilhada de caminho. Também observamos características específicas dos eventos de bloqueio para as duas estratégias de proteção.

Na maioria das redes simuladas, a razão da taxa de bloqueio entre proteção compartilhada e proteção dedicada ficou em torno de 0,5. Em algumas redes a diferença foi ainda maior, chegando a uma razão de 0,3. Quanto à utilização de recursos, não verificou-se uma diferença considerável entre as duas estratégias de proteção, do ponto de vista absoluto de utilização de recursos. Porém, ao avaliar os efeitos sobre a taxa de bloqueio, fragmentação e carga da rede, percebeu-se que o impacto foi grande. A fragmentação com proteção dedicada chegou a 0,8 em algumas redes, enquanto que, na proteção compartilhada, a fragmentação máxima foi de 0,6. Algumas redes apresentaram fragmentação entre 0,3 e 0,5. Além disso, as redes Memorex, Metrona e RNP tiveram aumento da carga média suportada em quase 50% com o uso de proteção compartilhada.

Estes resultados nos permitem afirmar que a proteção dedicada compromete a rede de uma forma muito mais impactante do que a proteção compartilhada e necessita de um conjunto maior de recursos para manter uma performance equivalente.

Palavras-chave: Redes ópticas elásticas. Bloqueio em redes ópticas. Sobrevivência em redes ópticas. RMLSA.

ABSTRACT

A blocking in optical networks is an event where a requested is not established due to network unavailability of resources. It is often used as a parameter for evaluate the network performance. A high blocking rate indicates that the network is not suitable for a given traffic demand.

Survivability is a characteristic of actual telecommunication networks, which allow the operation even in the event of link or node failures. In order to a network survive, spare capacity is employed to avoid blocking.

The amount of spare capacity must be planned in order to cope with the expected performance, costs of maintenance, complexity of control and capital expenditure.

In the recent Elastic Optical Networks, the routing and spectrum assignment problem evolved to a more complex problem, that is the routing, modulation and spectrum assignment. This problem imposes new constraints to the traffic engineering task.

In this work we investigated the relationship between protection strategies to the network with other properties affected by it. We compare the blocking rate and resource utilization rate considering both shared and dedicated protection strategies. Furthermore, we analyze special characteristics of the blocking events to both type of protection.

In the most of simulated networks, the blocking rate of the shared protection was around 0,5 of the dedicated protection. In some cases, the rate was 0,3. With respect to the resource utilization there is not a considerable difference between two strategies, in a absolute perspective. However, bringing the comparsion to blocking rate and link fragmentation, we saw that the impact was very significant. With the dedicated protection, some networks was a fragmentation around 0,8, while in shared protection the fragmentation was around 0,6, 0,5 and 0,3. Using shared protection, the networks Memorex, Metrona and RNP was average load increased by around 50% in comparsion to dedicated protection.

These results allow us say that dedicated protection causes a high impact in the network and requires a large amount of resources to allow a equivalent performance.

Keywords: Optical networks, Elastic networks, Blocking, Survivability, Protection, Routing, Spectrum assignment, Block rate, Spectral efficiency.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A disponibilidade é um aspecto crítico em uma rede de telecomunicações. Quando a rede não pode atender uma solicitação de conexão, tem-se um evento de bloqueio. O bloqueio é sempre causado pela incapacidade momentânea da rede de atender tal requisição, pela insuficiência de recursos. Nas situações de falha, a possibilidade de bloqueio na rede aumenta por que alguns recursos ficam temporariamente inutilizados.

A sobrevivência é a característica que a rede apresenta de manter a possibilidade de conexão entre quaisquer nós, mesmo em situações de falhas. Por sua vez, a sobrevivência pode impactar negativamente no bloqueio, por que compromete recursos da rede especificamente para trabalhar em situações de falha, deixando-os ociosos na maior parte do tempo.

Em termos construtivos da rede, a sobrevivência é provida pela simples existência de dois caminhos disjuntos entre quaisquer pares de nós. No entanto, no seu funcionamento, há vários outros aspectos que interferem na sobrevivência, tais como a estratégia escolhida para roteamento do tráfego e para realocação durante falhas, a estrutura topológica e o perfil das demandas de tráfego que, por sua vez, também são itens tocantes ao projeto.

A sobrevivência permite que, em situações de falha, a rede mantenha a disponibilidade de serviço para as conexões alocadas e para eventuais novas conexões alterando temporariamente as rotas convencionais, de acordo com a estratégia definida e reestabelecendo o roteamento habitual após a correção da falha.

Com o surgimento das redes óticas elásticas (*Elastic Optical Networks* - EONs), cuja proposta fundamental é permitir que o espectro de frequências onde trafegam os dados seja utilizado de forma mais eficiente, surgem novos elementos na estrutura, operação e controle da rede. Além das inovações tecnológicas (i.e., novos formatos de modulação, transponders de configuração variável por software, equipamentos mais robustos e potentes etc) a arquitetura das redes elásticas é mais complexa. Nela, a unidade de alocação do espectro ótico apresenta menor granularidade do que na arquitetura fixa tradicional. Isto possibilita o seu uso mais eficiente, ou seja, menos desperdício de espectro ao criar o *lightpath*[1], que é o caminho para tráfego do sinal.

Esta vantagem, porém, traz um efeito negativo que é a fragmentação do espectro. Diz-se que o espectro está fragmentado quando a sua ocupação está distribuída por toda a faixa de frequência, com lacunas entre as faixas ocupadas (ROSA et al., 2015). Por sua vez, a fragmenta-

[1] Caminho de luz: termo específico para redes ópticas. Também é possível utilizar o termo "canal" para referir-se ao $lightpath$, embora este seja mais genérico.

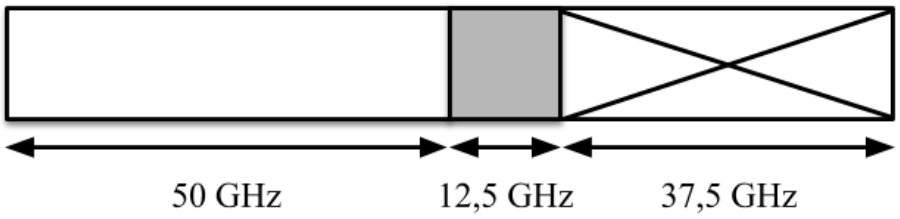

Figura 1.1 – Rede Fixa com $Slots$ de 50 GHz

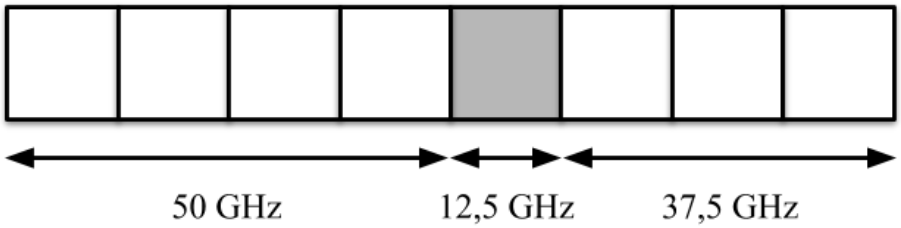

Figura 1.2 – Rede Elástica com $Slots$ de 12,5 GHz

ção é um evento potencializador do bloqueio, por que afeta diretamente as duas restrições mais básicas da atribuição de espectro em redes elásticas, que são a continuidade[2] e a contiguidade[3].

Nas redes convencionais o espectro é dividido em *slots*[4] de 50 ou 100 GHz e o $lightpath$ é alocado sobre estes *slots* fixos, causando grande desperdício da faixa de frequência alocada (CANDIA, 2014). A figura 1.1 mostra a divisão do espectro com um *slot* de rede fixa alocado para uma demanda de 12,5 GHz, causando um desperdício de 37,5 GHz (75% da frequência do *slot*).

Já nas redes elásticas, o $lightpath$ pode ser alocados sobre *slots* cujo tamanho é um múltiplo de 12,5 GHz, utilizando-se tantos *slots* quantos forem necessários. A figura 1.2 mostra um *slot* de uma rede elástica alocado para uma demanda de 12,5 GHz, ou seja, utilizando integralmente o espectro disponível. Além disso, as redes elásticas têm a capacidade inerente de alocação de *super-lightpaths* ou supercanais (canais na ordem de 400 GHz e 1 THz).

Nesta comparação temos uma situação ideal para a rede elástica, ou seja, a demanda é exatamente um múltiplo do tamanho do *slot*. A mesma vantagem não ocorreria com a rede fixa, ainda que houvesse uma demanda de 50 GHz, pois uma rede elástica também poderia alocar tal faixa de espectro sem nenhum desperdício.

---

[2] A mesma faixa de frequência deve estar disponível em toda a rota.

[3] A faixa de frequência necessária deve estar disponível em *slots* adjacentes.

[4] Embora usemos o termo *slot* para falar de redes fixas, este termo ficou convencionado com o surgimento das redes elásticas. No entanto, independente do contexto, sempre que falarmos em *slot* , estamos falando de uma faixa de frequência de tamanho específico, ou seja, a unidade de alocação.

2 OBJETIVOS

2.1 Objetivos gerais

Avaliar os impactos do uso de proteção dedicada e compartilhada na ocorrência de bloqueio em redes ópticas elásticas de telecomunicações.

2.2 Objetivos específicos

- Identificar aspectos relevantes afetados pelo uso de proteção dedicada ou compartilhada;
- Avaliar a diferença no desempenho e utilização de recursos da rede a partir de métricas como taxa de bloqueio, eficiência espectral, fragmentação, quantidade e razão de recursos para proteção.
- Caracterizar a ocorrência de bloqueio a partir de propriedades específicas.

3 JUSTIFICATIVA

Nas tradicionais de grade fixa ou WDM (*Wavelength-division Multiplex*), era necessário apenas alocar um determinado comprimento de onda (canal) para transporte dos dados, bastando que tal faixa de frequência estivesse disponível em todo o caminho desejado, satisfazendo a restrição de continuidade. Nas redes ópticas elásticas surgem novas restrições para o problema da atribuição de rota.

Nesta nova arquitetura, o principal agravante para o problema é cumprir a restrição de contiguidade, ou seja, todo o espectro necessário para alocação do *lightpath* deve estar disponível em *slots* de frequência adjacentes. Além desta restrição, a continuidade se torna mais complexa, pois se um único *slot* não estiver disponível em todo o caminho que se pretende utilizar, a alocação não poderá ocorrer.

A distância pela qual o sinal pode ser enviado sem sofrer atenuação que comprometa sua interpretação depende do formato de modulação usado e é outro fator que interfere significativamente nas restrições comentadas acima. Estas novas características das redes elásticas podem aumentar significativamente a taxa de bloqueio de uma rede.

4 TRABALHOS RELACIONADOS

Com o advento das redes ópticas elásticas, muitos trabalhos surgiram com a inteção de avaliar a melhoria de performance da nova arquitetura em relação à arquitetura de grade fixa tradicional. Um deles é o trabalho de VELASCO et al. (2012), em que são reportadas as principais contribuições e questões de interesse da comunidade envolvida, desde operadores de redes até o meio acadêmico científico.

De forma geral, a maioria dos trabalhos aborda inicialmente a proposta de melhoria de performance e a implicação de novas técnicas de controle, custo da rede, custo de operação, limitações físicas etc...

Um trabalho muito significativo e que, de certa forma, foi nosso ponto de partida, é o trabalho de SHEN; GUO; BOSE (2016), onde é feito um apanhado de propostas de métodos de sobrevivência para redes ópticas elásticas. Este trabalho faz a análise de uma série de aspectos afetados pelos métodos de roteamento, enquanto o nosso pretende comparar os efeitos causados pela estratégia de sobrevivência avaliando métricas específicas como taxa de bloqueio, carga, fragmentação e comprometimento dos recursos da rede.

O trabalho de KLINKOWSKI et al. (2013) aborda, principalmente, a variação do cenário de demandas de tráfego em uma rede e como ela pode se adequar aos diferentes perfis (horários de pico, de uso moderado, finais de semana etc...). Esta dinamicidade é uma das causas mais fortes da evolução das redes ópticas para a arquitetura de grade elástica.

O trabalho de SATKUNARAJAH; KRISHANTHMOHAN; RAGEL (2015) aborda diretamente o assunto da sobrevivência, propondo um método híbrido baseado em proteção com compartilhamento limitado de recursos.

Em MARINO; DELGADO; ZARAGOZA (2015) é avaliada a necessidade de tamanho do banco de transponders reconfiguráveis para tornar a taxa de bloqueio insignificante.

Em ROSA et al. (2015) também se faz uma avaliação dos eventos de bloqueio em função da indisponibilidade de recursos e da fragmentação.

Já o trabalho de (TESSINARI et al., 2016) serviu de orientação para construção da ferramenta de simulação que utilizamos neste trabalho, assim como a ferramenta de simulação desenvolvida por (MOURA; DRUMMOND, 2018).

É importante dizer que, além dos trabalhos aqui citados, há uma vasta quantidade de trabalhos relacionados ao assunto e muitos outros dos quais tomamos conhecimento ao longo

deste. No entanto, os trabalhos aqui citados dão uma cobertura adequada ao estudo que fizemos. Ainda, servem para mostrar como o assunto é amplo e como este e outros trabalhos podem ser evoluídos diante do tamanho do universo abrangido pelo tema.

5 ROTEAMENTO E ATRIBUIÇÃO DE ESPECTRO

O problema de encontrar recursos não ocupados (i.e. *slots* de frequência) do espectro óptico para estabelecer um caminho para uma demanda de tráfego é conhecido como propblema do Roteamento e Atribuição de Espectro ou RSA (*Routing and Spectrum Assignment*)(KLINKOWSKI et al., 2013). Nas redes ópticas este caminho é chamado, de maneira mais específica, de $lighpath$, ou seja, o caminho de luz pelo qual o sinal será enviado. O problema do RSA é a evolução do problema do Roteamento e Atribuição do Comprimento de Onda ou RWA (*Route And Wavelength Assignment*) das redes de grade fixa. Mais especificamente, o RSA também compõe o problema do Roteamento, Modulação e Atribuição de Espectro ou RMLSA (*Routing, Modulation Level and Spectrum Assignment*).

5.1 Continuidade e contiguidade

Nas redes fixas tradicionais, o problema da alocação de rota continha apenas a restrição de que a frequência a ser alocada deveria estar disponível em toda extensão do caminho desejado.

Já nas redes elásticas, as restrições se tornaram mais severas. É necessário que a faixa de espectro desejada esteja disponível num conjunto de *slots* adjacentes e que este conjunto esteja disponível em todo o caminho desejado.

Na figura 5.1, temos uma situação que impede o atendimento de uma requisição que demande 3 *slots* nos $links$ 0 a 3. Neste caso, a restrição de continuidade está violada. Nos $links$ 0 e 1, o bloco de *slots* 2:6 está disponível, enquanto que nos $links$ 2 e 3, o bloco 0:3 está disponível. Isto impede que o $lightpath$ seja alocado na mesma faixa de espectro. Seria possível atender, no entanto, uma demanda de 2 *slots* no bloco 2:3. Da mesma forma, é possível atender uma demanda de 5 *slots* nos links 0 e 1, alocando o bloco 2:6, assim como uma demanda de 4 *slots* nos links 2 e 3, alocando o bloco 0:3.

Vale observar que a restrição de contiguidade é uma restrição avaliada de forma indireta, uma vez que a disponibilidade do primeiro $link$ obriga a disponibilidade nos demais $links$ da rota, do contrário, a própria restrição de continuidade já é violada. Por isto, os algoritmos de atribuição não têm a perspectiva de indicar se há contiguidade no $link$, pois ela é inerente à continuidade. A exceção ocorre quando o primeiro $link$ do caminho não apresenta recursos disponíveis, caso em que o bloqueio pode ser dar pela falta de contiguidade ou mesmo por

exaustão do $link$.

Estas características podem fazer com que a rede fique fragmentada após um tempo de operação. Ou seja, a sequência de alocações e liberações de espectro, podem resultar em uma situação de muitos *slots* ou blocos de *slots* não utilizados espalhados e que terão pouca probabilidade de serem alocados. Políticas de desfragmentação do espectro são outro objeto muito importante de estudo na engenharia de telecomunicações.

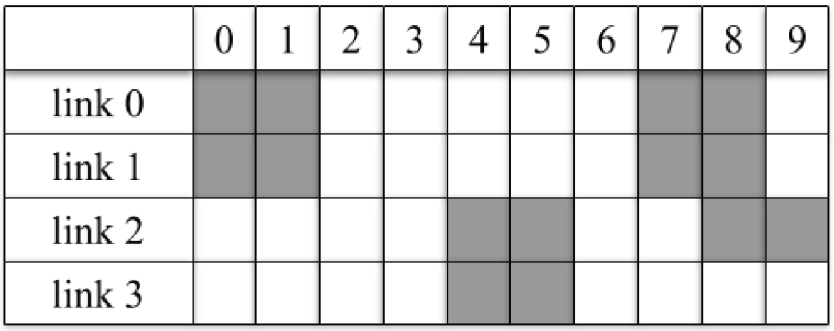

Figura 5.1 – Conjunto de 4 $Links$ com Alguns Blocos de $Slots$ ocupados

5.2 Bloqueio

O evento de uma requisição não atendida pela indisponibilidade de recursos da rede é chamado de bloqueio e pode ocorrer com maior ou menor frequência, dependendo das técnicas utilizadas para o RMLSA.

O principal apelo das redes óticas elásticas é diminuir a probabilidade de bloqueio das demandas, criando a possibilidade de alocar canais mais adequados a cada demanda de tráfego, aumentando a eficiência de utilização do espectro óptico.

As situções mencionadas na seção 5.1 são ilustrações de bloqueio, ou seja, quando não é possível alocar recursos suficientes para atender a requisição recebida.

A taxa de bloqueio de uma rede é a razão entre a quantidade de requisições que não puderam ser atendidas de imediato, devido a indisponibilidade de recursos, e o total de requisições da rede. Esta taxa pode ser calculada em qualquer instante t de forma parcial ou total. As expressões que fornecem a taxa de bloqueio são:

$$TBP_t = \frac{RB_t - RB_{ta}}{RT_t - RT_{ta}} \tag{5.1}$$

$$TBT = \frac{RB}{RT} \tag{5.2}$$

Onde:

- TBP: taxa de bloqueio parcial[5];
- TBT: taxa de bloqueio total;
- RB: quantidade de requisições bloqueadas;
- RT: quantidade total de requisições;
- t: tempo;
- ta: tempo anterior;

As expressões aqui apresentadas foram baseadas nas expressões utilizadas por (TESSINARI, 2016).

5.3 Eficiência espectral

A eficiência espectral é a razão entre a faixa de espectro necessária para envio dos sinais e a faixa de espectro alocada. Nos casos onde a demanda é um múltiplo do tamanho do *slot*, a eficiência espectral atingirá um valor ótimo. Já nos demais casos, sempre haverá um desperdício de frequncia. No entanto, mesmo nestes casos, a eficiência espectral aumenta consideravelmente, devido à nova convenção de tamanho do *slot* das redes elásticas, sobretudo em função das demandas que requerem menor faixa de espectro.

As expressões que fornecem o valor da eficiência espectral são:

$$EE(r) = \frac{FN(r)}{FA(r)} \tag{5.3}$$

$$EE = \frac{FN}{FA} \tag{5.4}$$

Onde:

- EE: Eficiência espectral;
- FN: Frequência necessária;
- FA: Frquência alocada;
- r: requisição;

[5] Taxa de bloqueio considerando um intervalo de tempo.

As expressões para calcular a eficiência espectral foram baseadas nas expressões do cálculo da taxa de bloqueio.

Neste trabalho, as simulações terão um padrão de tráfego para as requisições. Por isto, o cálculo da eficiência espectral pode ser feito de forma genérica para cada taxa de tráfego requisitada. Isto está melhor apresentado e detalhado na seção 8.3 do capítulo 8.

6 SOBREVIVÊNCIA EM REDES ÓPTICAS

A sobrevivência de uma rede é a sua capacidade de manter a conexão entre quaisquer nós, mesmo em situações de falha. Esta é uma questão crítica, sobretudo em redes de alta largura de banda e com topologia arbitrária.

As redes óticas estão sujeitas aos mais variados tipos de danos, de forma que falhas são vistas como fatos inevitáveis (ELLINAS et al., 2016). As redes podem ser afetadas por fenômenos naturais, manutenção de outras redes próximas, como redes de energia elétrica, choques de veículos, incêndios, ação de escavadeiras e alagamento (redes subterrâneas).

Estas redes carregam volumes muito altos de dados e assim, caso um recurso apresente falha, o número potencial de usuários afetados é grande.

Os métodos de sobrevivência consistem em prover uma alternativa de rota para o tráfego de dados quando ocorrem as falhas. A alternativa pode ser fim a fim (caminho completo) ou apenas em parte do caminho afetado.

Buscando o melhor compromisso com prioridade para algum aspecto, as técnicas de sobrevivência são desenvolvidas com base em diversas abordagens e são mais amplamente classificadas em técnicas de proteção e restauração.

As técnicas baseadas em proteção possuem um plano pré-definido para prover a sobrevivência, enquanto as técnicas baseadas em restauração definem tal plano no momento de ocorrência da falha. O compromisso destas duas abordagens é entre complexidade do tratamento de falhas, garantia e velocidade de recuperação da rede e eficiência de utilização dos recursos. Na abordagem de proteção, muitos recursos da rede são reservados apenas para prover a alternativa para o tráfego em caso de falha. Com isto, tem-se uma resposta mais breve da rede, porém haverá sempre um alto índice de comprometimento de recursos para sobrevivência. Já nas técnicas baseadas em restauração, os recursos da rede podem ser amplamente utilizados em condições normais e serem alocados para recuperação apenas durante as situações de falha.

De forma geral, os métodos de sobrevivência podem ser baseados em enlace e caminho:

- Enlace: apenas o enlace é protegido ou recuperado por um segmento. Esta abordagem é bastante complexa, pois impõe que qualquer caminho de tráfego afetado por uma falha tenha um segmento realocado. A recuperação ou proteção de um enlace sempre é feita por um segmento, uma vez que as redes possuem apenas um cabo entre dois nós.
- Caminho: a proteção ou recuperação ocorre de fim a fim, ou seja, caso ocorra alguma

falha no caminho, o tráfego é reenviado, a partir do nó de origem, por um caminho que é disjunto por enlace do caminho original. Esta é uma abordagem bastante simples e poderosa e amplamente utilizada.

Chamamos de caminho de trabalho o caminho principal por onde o tráfego é enviado inicialmente e chamamos de caminho de proteção (ou de *backup*), o caminho alternativo, por onde o tráfego será enviado em caso de falha de algum enlace do caminho principal. Nestes casos, um requisito geral para a sobrevivência é que o caminho de proteção seja disjunto por enlace do caminho de trabalho, como mostra a figura 6.1. Caso contrário, se uma falha ocorresse em um dos enlaces comuns aos dois caminhos, o caminho de proteção também estaria afetado e não poderia ser usado. Por outro lado, caminhos de proteção não são, necessariamente, disjuntos por enlace entre si. Na figura, os caminhos de trabalho e proteção aparecem destacados com tracejado e pontilhado, respectivamente.

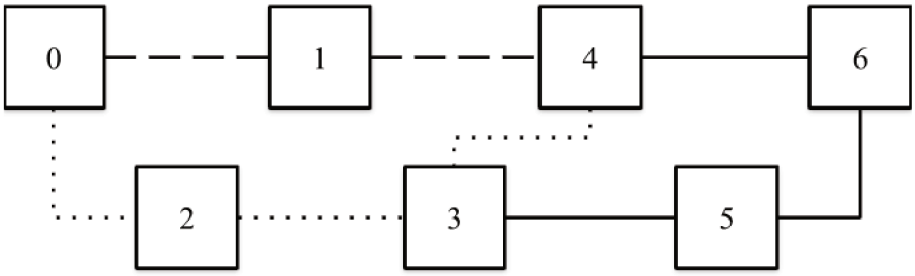

Figura 6.1 – Caminhos de Trabalho e Proteção

A escolha do método de sobrevivência tem impacto direto no custo de capital ($CapEx$) da rede e outros aspectos. Como já mencionado anteriormente, há sempre uma propriedade favorecida em face de outra. O uso de abordagens reativas e compartilhadas proporciona maior eficiência de utilização dos recursos (EIRA et al., 2014), enquanto as abordagens protetivas e dedicadas proporcionam mais garantia e rapidez de resposta no tratamento da falha.

A figura 6.2 mostra uma divisão geral das técnicas de proteção. A maioria das abordagens permitem proteção e restauração por caminho ou por enlace. No entanto, algumas técnicas são especialmente definidas para uma abordagem específica, como a de recuperação de enlace (*Span Restoration*), e outras são híbridas, como a de Backup Pré-definido com Compartilhamento Limitado (PBPRLS), proposta por (SATKUNARAJAH; KRISHANTHMOHAN; RAGEL, 2015).

Também é comum que a proteção seja referida por nomes como 1:1, N:1 ou 1+1. Nesta convenção, os termos representam a quantidade de caminhos para proteção e trabalho. Outros

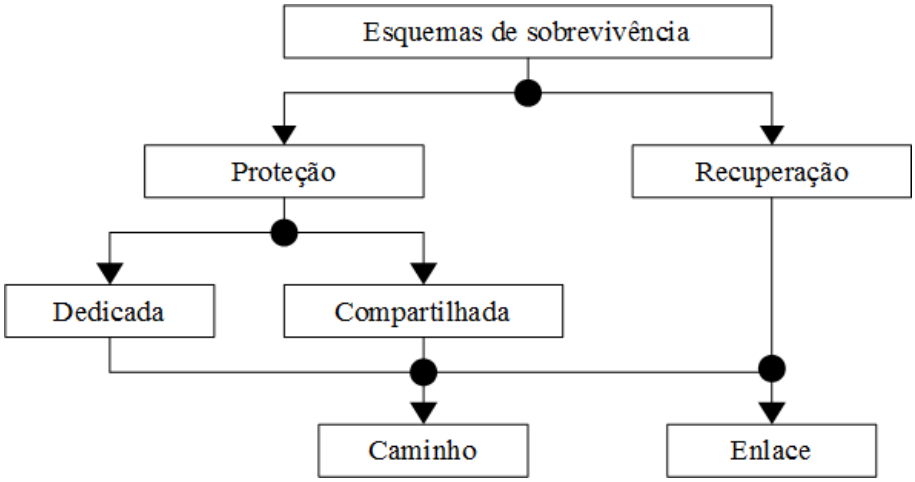

Figura 6.2 – Classificação das Técnicas de Sobrevivência

termos e expressões muito encontrados na literatura são "proteção reativa", "proteção $online$", "restauro" e "recuperação", para sobrevivência baseada em recuperação e "proteção *offline*", "proteção pró-ativa" e "proteção preventiva" para sobrevivência baseada em proteção.

6.1 Métodos de Proteção Compartilhados

Nos métodos baseados nesta abordagem, os recursos utilizados por caminhos de proteção são compartilhados. Embora se tenha uma cobertura menor sobre as falhas, esta opção é mais eficiente sob o ponto de vista de utilização dos recursos da rede. Para este tipo de proteção faz-se necessário que os caminhos protegidos sejam disjuntos por enlace. Assim fica garantido que em nenhuma falha simples em apenas um dos caminhos protegidos haverá bloqueio de demanda, desde que as demais restrições de alocação estejam satisfeitas.

A figura 6.3 mostra um exemplo de dois caminhos de proteção (P1 e P2) protegendo dois caminhos de trabalho (T1 e T2), respectivamente. Os caminhos P1 e P2 compartilham os *slots* 0:3 no enlace 3-4.

O principal apelo dos métodos compartilhados é o uso eficiente dos recursos da rede, diminuindo a necessidade de recursos adicionais. Por outro lado, o controle de roteamento do tráfego e alocação do espectro em caso de falhas se torna mais complexo.

6.2 Métodos de Proteção Dedicados

Por outro lado, nos métodos dedicados, há um caminho de proteção exclusivo para cada caminho de trabalho, o que gera a necessidade de grande quantidade de recursos, em boa parte

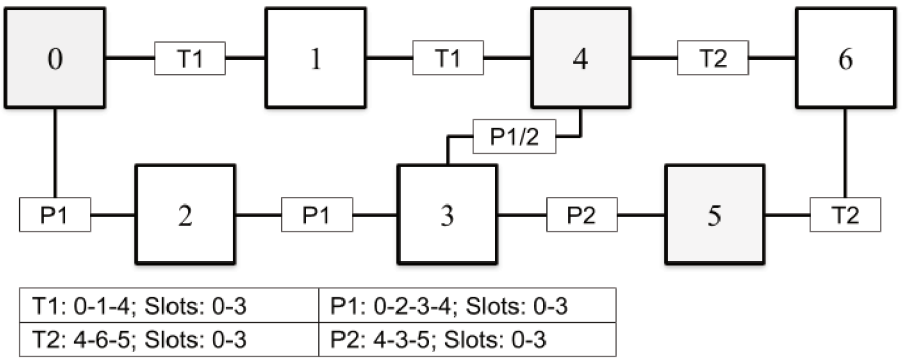

Figura 6.3 – Proteção Compartilhada

do tempo, não utilizados. Simplesmente devido à estrutura do esquema de proteção, a utilização da rede é de, no máximo, 50%, mas na prática é sempre menor, pois os caminhos de backup são, em média, mais longos que os caminhos de trabalho.

Na figura 6.4 temos os caminhos de proteção P1 e P2 protegendo os caminhos de trabalho T1 e T2, respectivamente, sendo que P1 e P2 não compartilham recursos (P1 está alocado nos *slots* 0:3, enquanto P2 está alocado nos *slots* 4:7).

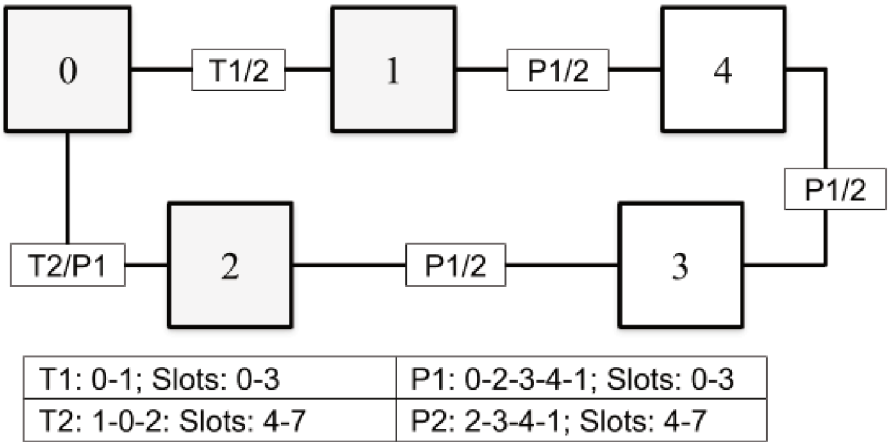

Figura 6.4 – Proteção Dedicada

Apesar de impor um custo maior ($CapEx$), esta abordagem fornece muito mais tolerância à falhas, além de exigir menor custo de operação ($OpEx$). Em geral, após o restabelecimento de uma falha, o tráfego afetado por ela retorna para o seu caminho de trabalho, pois este caminho tende a ser mais curto.

Mais amplamente, a decisão de adotar um ou outro tipo de método depende do cenário de falha esperado para a rede e também do orçamento para implantação. Nos casos onde a probabilidade de ocorrer muitas falhas simultâneas é muito baixa, a proteção compartilhada é adotada devido ao fator de utilização. De forma geral, segundo (YUAN; JUE, 2003), os métodos

dedicados são utilizados para caminhos específicos que apresentam maior vulnerabilidade.

A proteção dedicada permite ainda uma solução mais ambiciosa (MORAIS, 2008), chamada de *dual-feeding* (1+1), onde o tráfego é enviado simultaneamente por dois caminhos, não havendo efetivamente um caminho de trabalho e outro para proteção. Um aspecto negativo dessa abordagem é o consumo excessivo de energia.

Os caminhos de proteção dedicados eventualmente irão proteger caminhos de trabalho que não são disjuntos, porém isso não pode ser confundido com o fato de o caminho de proteção não ser disjunto (caso da abordagem compartilhada).

7 SIMULADOR

7.1 Apresentação

Para efetuar as simulações pretendidas, foi desenvolvida uma ferramenta contendo os recursos específicos necessários. Tal iniciativa deveu-se a escassez de simuladores para redes óticas elásticas disponíveis para uso público e da inadequação daqueles que foram encontrados.

Alguns destes simuladores, embora com boa sofisticação, não atendiam as necessidades do nosso estudo e careciam de muitas modificações para torná-los adequados. A principal característica ausente dentre os simuladores verificados foi a opção de proteção compartilhada. Assim, desenvolvemos este novo simulador, que permite escolher o tipo de proteção, desta forma possibilitando a comparação dos efeitos do uso da proteção dedicada e compartilhada. Por estes motivos, a primeira versão de nossa ferramenta contém apenas os recursos básicos para simular o funcionamento de uma rede na perspectiva do nosso estudo.

De forma geral, ela possui semelhanças com outras ferramentas, no seu conceito e funcionamento. A simulação ocorre a partir da geração de requisições de conexão pseudo-aleatórias, as quais são roteadas e alocadas, de acordo com as técnicas implementadas ou escolhidas e da disponibilidade de recursos da rede.

A principal diferença desta ferramenta em relação as outras que encontramos é a opção de proteger as rotas de trabalho com rotas de proteção dedicadas ou compartilhadas, que é o foco do nosso estudo.

É necessário destacar que a implementação se baseou principalmente em outros dois simuladores que cogitamos utilizar em nosso estudo, a saber o Elastico++ (que é uma extensão do Omnet++) de (TESSINARI et al., 2016) e o Flexigrid 2.0 de (MOURA; DRUMMOND, 2018).

O fato de a ferramenta ser inicialmente simples não limita, no entanto, a sua evolução, nem seu uso para análises relacionadas, uma vez que a estrutura e o fluxo de funcionamento refletem objetos e eventos comuns numa rede de telecomunicações. Além disso, algumas opções são parametrizáveis, permitindo que vários cenários possam ser simulados.

Da mesma forma, novas funcionalidades, bem como novos algoritmos para o problema do RMLSA e outros recursos poderão ser facilmente adicionados à ferramenta no futuro. Esperamos que isto aconteça por nossa própria iniciativa e também de outras pessoas que venham a

utilizá-la.

7.2 Estrutura

A ferramenta está estruturada em 4 camadas principais, nas quais os itens e recursos estão agrupados de acordo com características de seu papel dentro do funcionamento da rede e também com características próprias de programação. São elas:

- $Core$: contém rotinas básicas da ferramenta, tais como a própria rotina de simulação e a rotina de gravação dos resultados.
- $Control$: contém objetos para controle do funcionamento da rede, tais como lista de rotas e lista de recursos alocados e disponíveis;
- $Modules$: contém objetos que criam eventos na simulação, tais como gerador de requisições e gerenciador de pedidos de conexão;
- $Statistics$: contém rotinas que coletam os dados da simulação;

7.3 Funcionamento

O funcionamento da simulação segue o fluxo da figura 7.1:

O primeiro evento na execução do simulador é a exibição da tela inicial, onde a simulação é parametrizada. Podem ser especificados alguns critérios e deve-se carregar as topologias das redes desejadas.

Depois de selecionar as opções desejadas, a simulação é executada. É feita uma simulação para cada uma das topologias. Também é possível repetir cada uma destas simulações num mesmo conjunto de execuções, sem a necessidade de rodar manualmente várias vezes cada simulação.

Esta funcionalidade facilita a comparação dos resultados de várias simulações de uma mesma rede com características variadas, ou ainda de várias simulações de diferentes redes com características iguais, dependendo na observação que se deseja fazer. Ao fixar o padrão de pseudo-aleatoriedade, em cada execução das simulações os valores influenciados por esse padrão serão os mesmos. Basicamente, estes valores são as características das requisições e conexões com nós de origem e destino, carga, tempo de permanência etc...

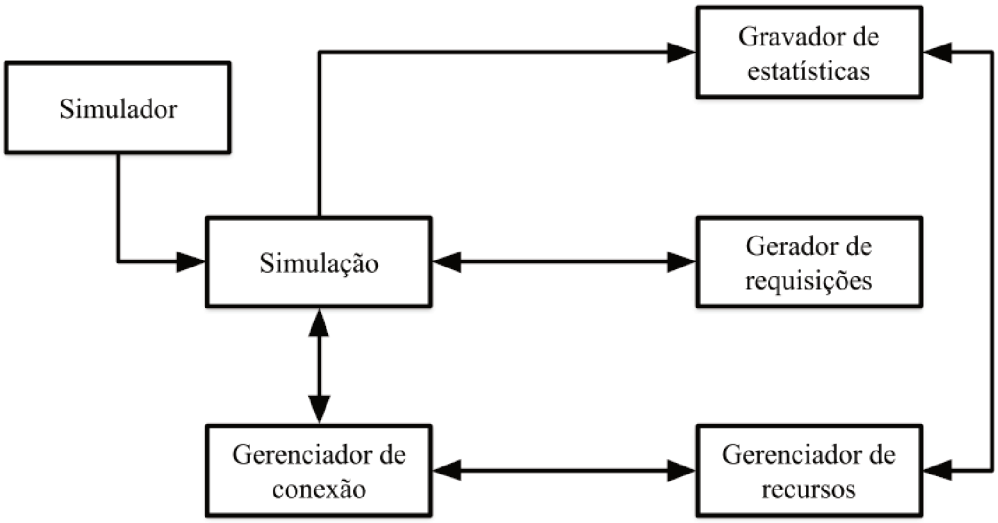

Figura 7.1 – Diagrama de Funcionamento do Simulador

Para cada execução das simulações, ocorre a seguinte sequência de eventos:

1. Leitura das topologias;
2. Inicialização dos componentes;
3. Geração das requisições pseudo-aleatórias;
4. Recebimento das requisições;
5. Consulta de rotas para alocação;
6. Verificação da disponibilidade de recursos;
7. Conexão aceita ou recusada;
8. Término da conexão após o tempo de permanência;
9. Gravação de resultados parciais;
10. Fim das requisições;
11. Liberação das conexões remanescentes na rede;
12. Gravação de resultados finais;

Os eventos de 3 a 9 são repetidos ciclicamente enquanto há requisições sendo geradas. São eles que compõem, a rigor, a simulação da operação da rede, ou seja, o conjunto de eventos

que acontecem durante uma situação normal de uso contínuo da rede: chegada de requisições e alocação ou bloqueio.

7.4 Padrões e parâmetros

Para descrever as topologias de rede, convencionamos uma estrutura específica em linguagem XML, onde o documento representa a rede e cada link é representado por um nó, conforme a imagem 7.2.

```
▼<network name="arnes" bidirectionalLinks="true">
  ▼<link id="1">
     <s>0</s>
     <t>1</t>
     <distance>100,165198199944</distance>
   </link>
  ▼<link id="2">
     <s>1</s>
     <t>2</t>
     <distance>24,3136621472108</distance>
   </link>
  ▼<link id="3">
     <s>2</s>
     <t>3</t>
     <distance>23,4236612626371</distance>
   </link>
```

Figura 7.2 – Estrutura do Arquivo de Descrição da Rede

Além da topologia, outras informações (variáveis) podem ser fornecidas ao simulador, para que execute as simulações com diferentes características. São eles:

- Número de execuções para cada simulação;
- Perfil de cargas ($bitrate$) das requisições;
- Distribuição do perfil de cargas;
- Número de requisições por simulação;
- Intervalo entre as requisições;
- Tipo de proteção;

As estatísticas da simulação são memorizadas a cada evento (requisição), porém a captura desses dados para gravação em uma saída ocorre apenas num intervalo definido. Os resultados finais são gravados ao término de todas as simulações.

Nesta primeira versão, a gravação dos resultados ocorre em arquivos de texto, em uma estrutura de séries, para facilitar a utilização destes dados na geração de gráficos em outras ferramentas.

Posteriormente, pretendemos criar formatos alternativos de gravação, bem como opções de quais dados se deseja gravar.

7.5 Algoritmos, políticas e controles

De acordo com nosso objetivo de estudo, adotamos o algortimo de Suurballe tradicional para roteamento. Já para a atribuição de espectro, adotamos as políticas *FirstFit* para o caminho de trabalho e *FirstLastFit* para o caminho de proteção. Dessa forma, as rotas selecionadas serão sempre as menores, tanto para trabalho quanto para backup, enquanto a ocupação do espectro em cada fibra ficará concentrada nas extremidades.

7.6 Tecnologias

A ferramenta ora descrita foi desenvolvida em linguagem C#, utilizando a plataforma .NET Framework com a IDE Visual Studio Comunity 2018.

7.7 Validação

Para validar a ferramenta, fizemos exaustivas repetições de simulação com os mesmos dados de entrada e, nessas ocasiões, os resultados obtidos foram os mesmos. Além disso, fizemos vários testes de consistência e mensagens de saída em console (modo verboso) para todas as instruções de rotinas crítcas, tais como leitura de topologia, descoberta de rotas, solicitação de conexão, verificação de disponibilidade de recursos, mapas de utilização dos $links$ após cada conexão iniciada ou finalizada etc...

No próximo capítulo, apresentamos os resultados das simulações feitas com as redes reais.

8 SIMULAÇÕES E DISCUSSÃO

As simulações que executamos neste estudo tiveram foco nas características de bloqueio apresentadas a partir do tipo de proteção (dedicada ou compartilhada).

O formato das simulações foi definido da seguinte forma:

- Foram selecionadas 12 topologias de redes reais: Arnes, CoxUsa, DeutschTelecom, Internet2Usa, MemorexEurope, Metrona UK, NFSNet, OmnicomEurope, RnpBrazil, UsaGde, Vbns e ViaDatacenterNet;
- Roteamento com o algoritmo de Suurballe (versão tradicional);
- Atribuição de espectro $FirstFit$ para a rota de trabalho e $FirstLastFit$ para a rota de proteção;
- 1000 requisições pseudo-aleatórias[6];
- Chegada das requisições à rede numa distribuição regressiva (maior frequência de pedidos no início da simulação, pelo fato de a rede estar inicialmente vazia);
- Tempo de permanência da conexão na rede entre 5 e 15 s;
- 320 *slots* de frequência de 12,5 GHz por link;
- Proteção dedicada e compartilhada (todas as simulações executadas para as duas abordagens);
- Padrão de carga das requisições (faixas de serviço) de 40, 100, 200 e 400 Gbps e 1 Tbps, distribuídos com uma probabilidade 5, 4, 3, 2, 1;

A partir do padrão de requisições estabelecido, foram geradas as quantidades de requisições para cada demanda conforme mostra a figura 8.1. A tabela 8.1 compara a proporção exata do padrão definido com a quantidade de requisições geradas.

8.1 Bloqueio

O objeto principal do resultado das simulações é um gráfico detalhado para cada rede simulada, que mostra a quantidade de bloqueios caracterizada e a carga atual, além de uma tabela comparativa com todas as redes, com informações resumidas.

Os gráficos com o resultado detalhado de cada rede usam como escala temporal a sequência de requisições, da primeira para a última. A informação referente a carga da rede

[6] Nos testes aqui apresentados a pseudo-aleatoriedade foi controlada com o uso da mesma semente.

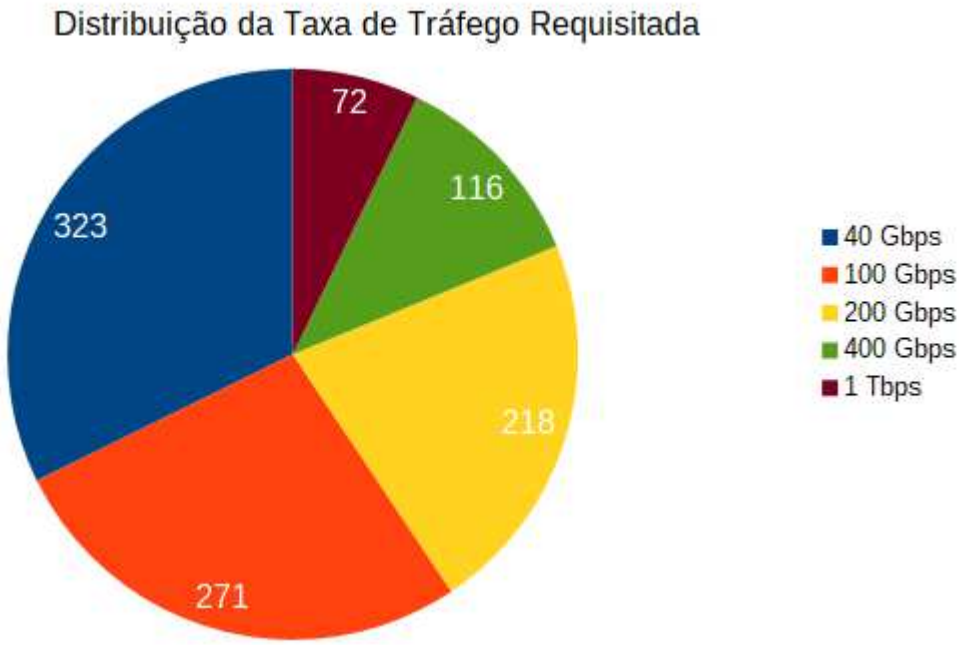

Figura 8.1 – Distribuição da Taxa de Tráfego das Requisições

Tabela 8.1 – Comparativo do Padrão de Distribuição com a Quantidade de Requisições Geradas

Taxa	Distribuição	Proporção	Quantidade exata	Quantidade gerada
40	5	0,33	333	323
100	4	0,27	267	271
200	3	0,20	200	218
400	2	0,13	133	116
1000	1	0,07	67	72
Total da distribuição			15	
Total de requisições			1000	

é pontual e as informações de bloqueio são acumuladas, pelo fato de o evento de bloqueio ser uma situação de baixa frequência em relação a quantidade de requisições recebidas pela rede. As informações são gravadas a cada evento da simulação, mas para adequar a quantidade de dados exibida e tornar possível a plotagem e leitura, selecionamos apenas 5 momentos desta coleção de estatísticas, exatamente a cada vigésima parte da simulação (200 requisições).

Uma das características inicialmente analisadas para o bloqueio, a exaustão da rota, não se mostrou significativa, havendo apenas 3 ocorrências nas redes Deutsch, Omnicom e Via Data Center. Isto indica que os enlaces da rota ainda possuíam *slot* disponível em todas as situações de bloqueio para a maioria das redes. Nos casos onde a disponibilidade de recursos era menor do que o necessário, temos uma situação comum de carga da rede próxima ao limite. Porém, nos casos onde os *slots* livres estavam apenas em posição inadequada para a alocação, tem-se uma situação de fragmentação do espectro, o que pode ser melhorado com outras técnicas não abordadas neste trabalho.

Nas simulações com proteção compartilhada, um fato importante é que não houve bloqueio no caminho de proteção. Isto faz sentido, pelo fato de que os recursos são compartilhados e isso gera uma menor utilização, ainda que a quantidade de enlaces necessária seja maior. Essa variação depende muito de aspectos da rede e do roteamento, mas diferentemente da proteção dedicada, onde a proteção sempre consome mais recursos que o caminho de trabalho, como vários recursos são compartilhados, o efeito prático é de menos recursos comprometidos no caminho de proteção do que no caminho de trabalho. Por este motivo, os gráficos não apresentam uma série com a quantidade de bloqueios na rota de proteção compartilhada.

Por outro lado, na maioria dos testes feitos com proteção dedicada, apenas cerca de metade dos bloqueios ocorreu no caminho de proteção. Isto ocorre por que a diferença de custo para o caminho de trabalho não é muito grande e só é possível pela topologia das redes que permitem rotas alternativas com tal diferença de custo.

O tráfego imposto à rede na simulação foi uma escolha que, num tempo adequado, leva as redes a ficarem sobrecarregadas, uma vez que o objetivo era justamente observar as características dos eventos de bloqueio.

A tabela 8.1 e os gráficos das figuras 8.3 a 8.14 mostram os resultados das simulações, respectivamente, com informações gerais resumidas e informações específicas detalhadas de cada rede.

Tabela 8.2 – Bloqueio, Carga e Utilização de Recursos por Rede

	Proteção Dedicada				Proteção Compartilhada			
Rede	**B**	**Cm**	**Rt**	**Rp**	**B**	**Cm**	**Rt**	**Rp**
Arnes	198	9774	43,57	68,36	107	13778	49,75	64,27
Cox	62	15328	24,27	61,65	24	18050	26,04	58,46
Deutsch	67	14968	34,6	59,72	29	17706	36,72	55,57
2 USA	195	9680	35,83	63,83	68	13284	40,38	61,21
Memorex	229	9444	35,34	66,94	87	15064	44,93	62,34
Metrona	193	9688	30,78	62,95	84	14324	37,98	60,5
NFSNet	81	13518	35,03	62,5	8	19344	39,81	55,79
Omnicom	89	13048	26,23	61,4	27	16968	30,41	57,87
RNP	176	10240	49,9	63,42	67	14296	56,3	59,24
GDE	37	15532	12,73	56,24	10	15868	13,06	53,89
VBNS	155	11828	38,43	62,48	70	16236	45,21	58,51
Via Data Center	158	11122	46,52	64,61	59	15368	52,01	60,08

Significado das abreviações	
B	Quantidade total de bloqueios
Cm	Carga pontual da rede (Gbps)
Rt	Percentual de recursos alocados para trabalho
Rp	Razão entre recursos alocados para proteção e o total

O gráfico da figura 8.2 e a tabela 8.1 comparam o bloqueio nas redes para proteção dedicada e compartilhada, além de mostrar a taxa de bloqueio (a quantidade de requisições bloqueadas em relação ao total de requisições) e a razão de bloqueio entre o uso de proteção compartilhada e dedicada.

As letras D e C entre parênteses nas legendas dos gráficos indicam, respectivamente,

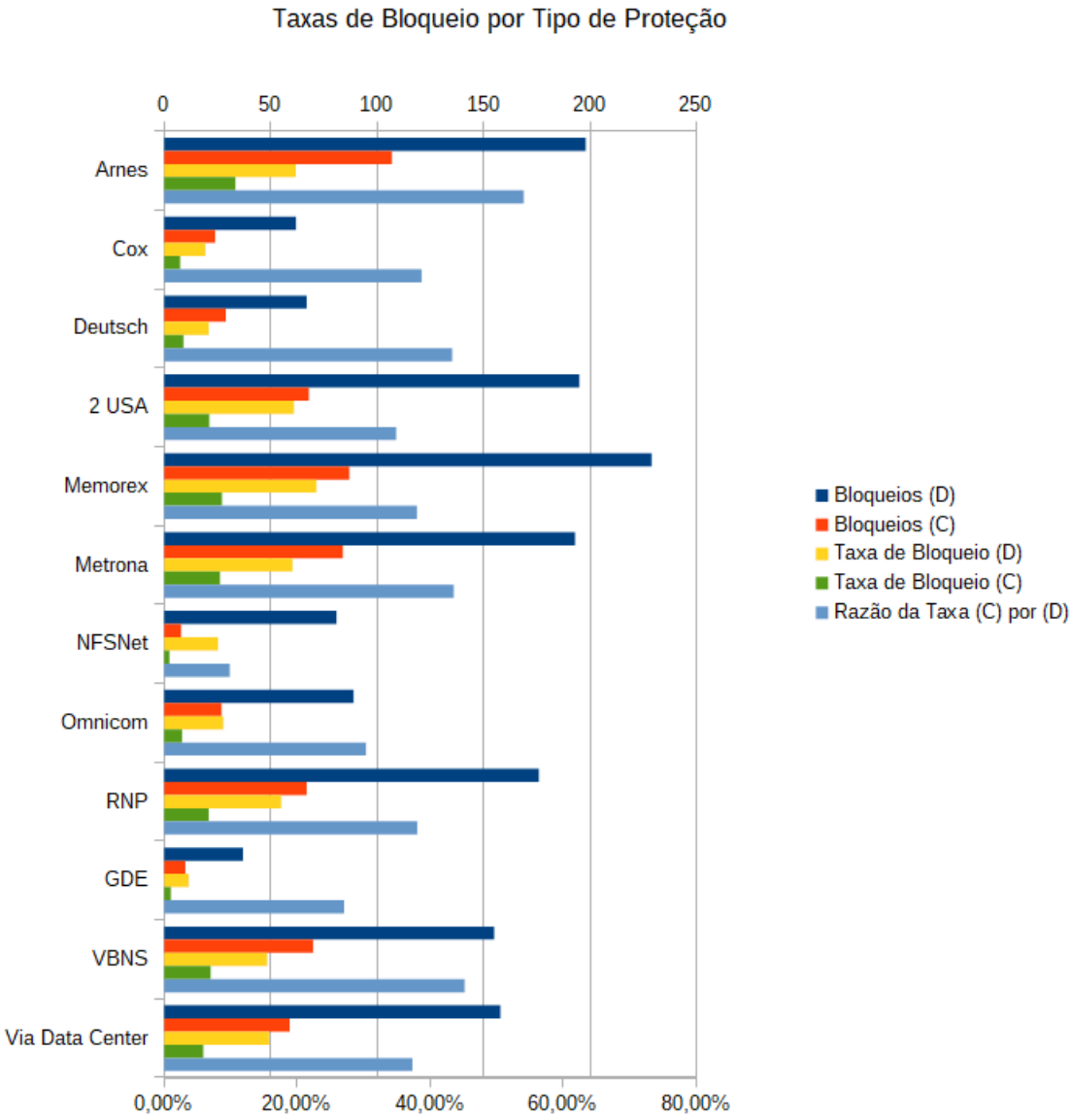

Figura 8.2 – Taxa de Bloqueio por Tipo de Proteção

proteção dedicada e proteção compartilhada.

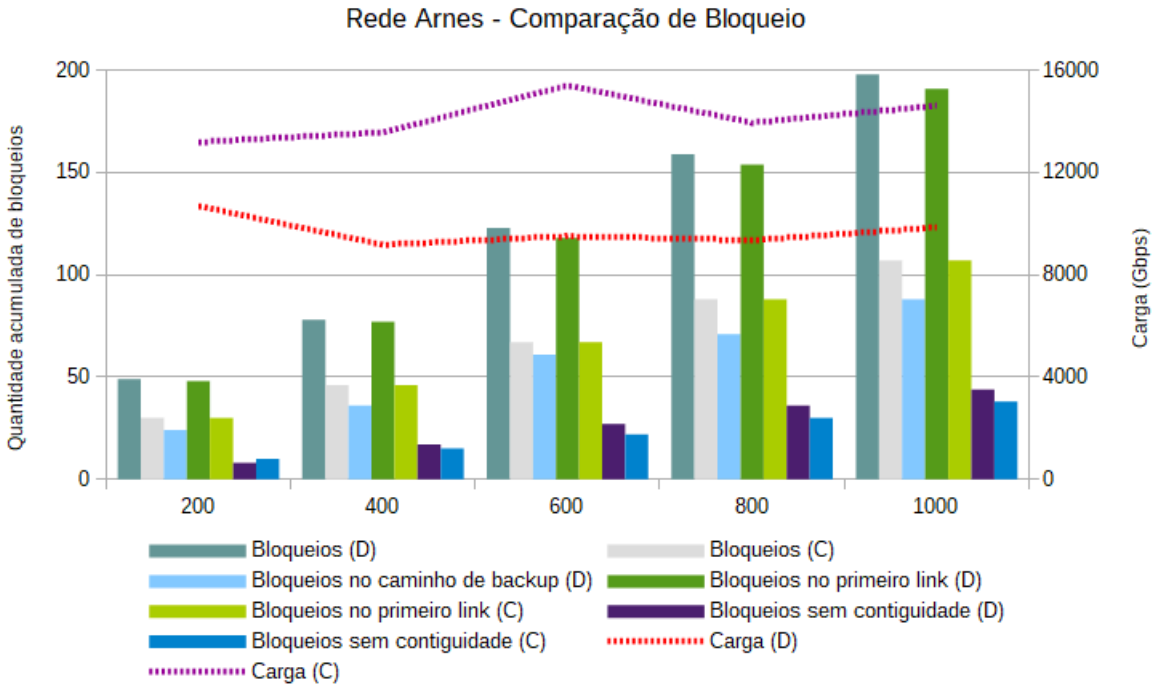

Figura 8.3 – Arnes - Comparativo de Carga e Bloqueio

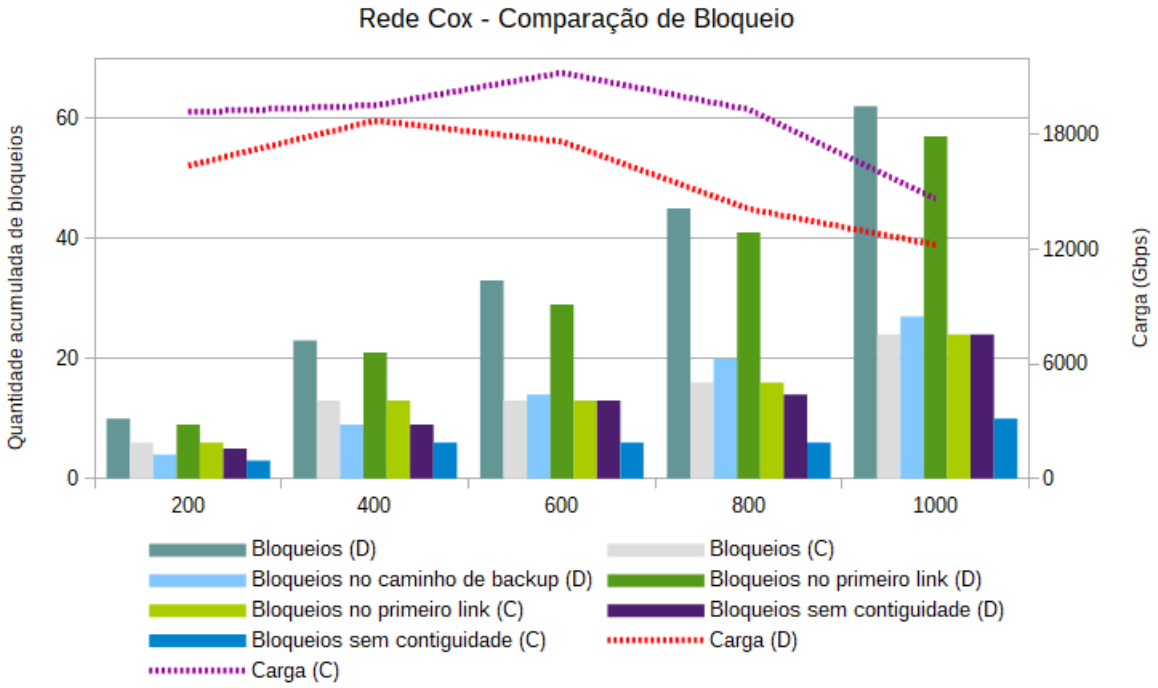

Figura 8.4 – Cox USA - Comparativo de Carga e Bloqueio

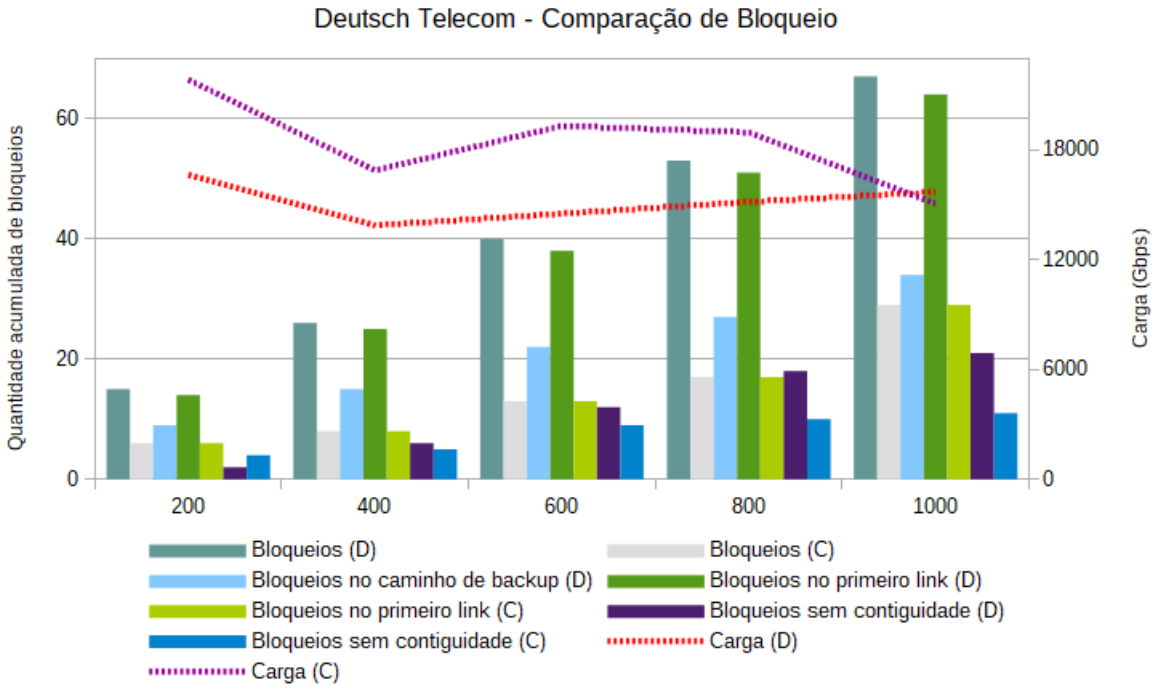

Figura 8.5 – Deutsch Telecom - Comparativo de Carga e Bloqueio

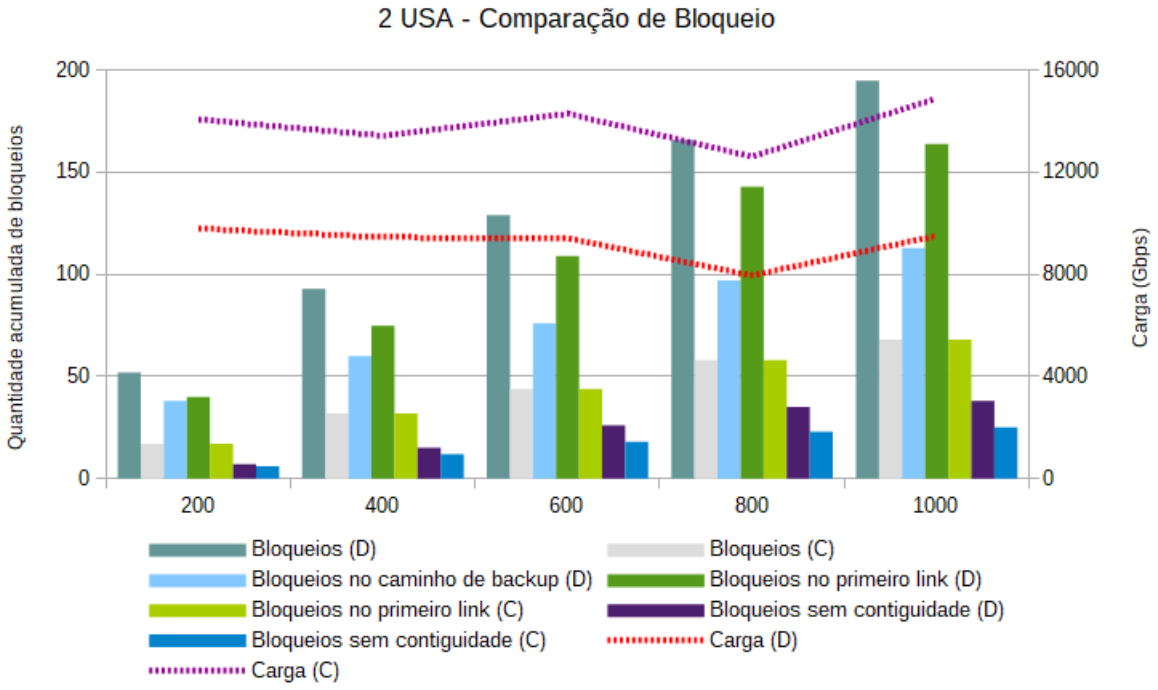

Figura 8.6 – 2 USA - Comparativo de Carga e Bloqueio

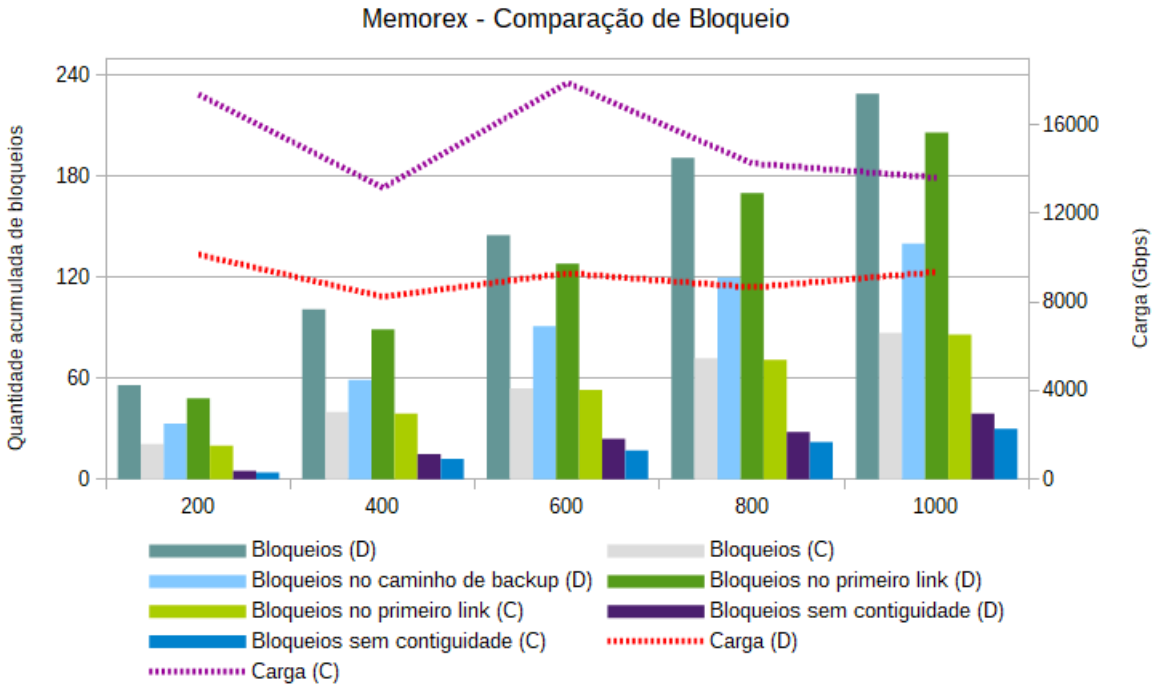

Figura 8.7 – Memorex - Comparativo de Carga e Bloqueio

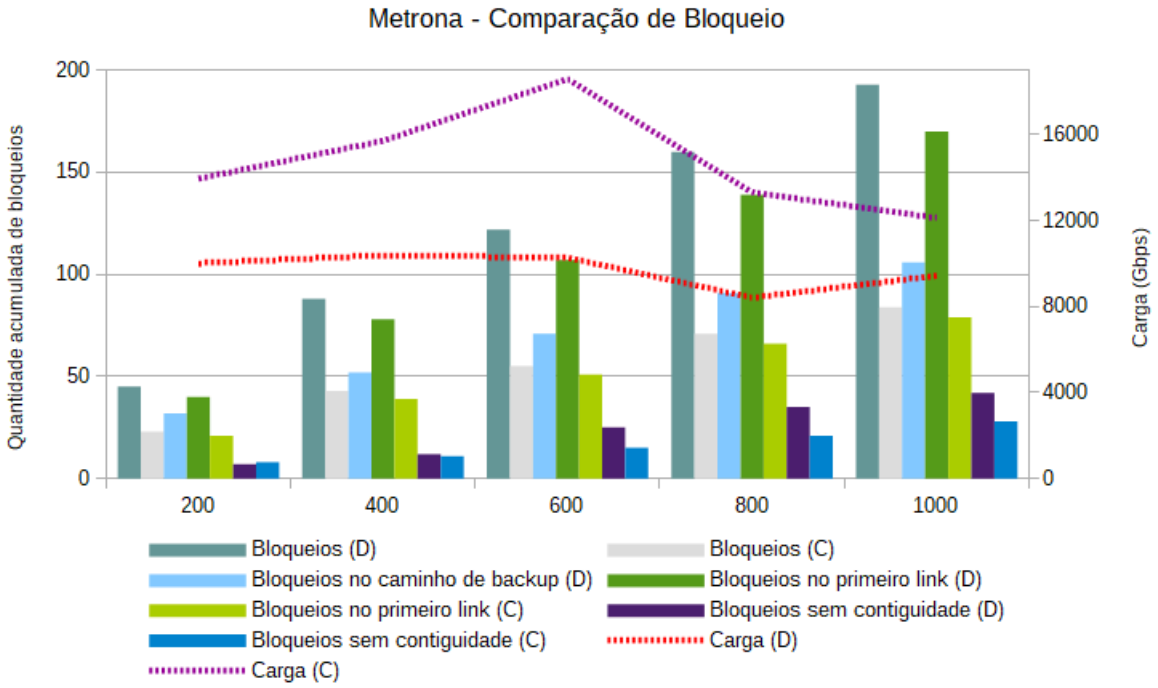

Figura 8.8 – Metrona - Comparativo de Carga e Bloqueio

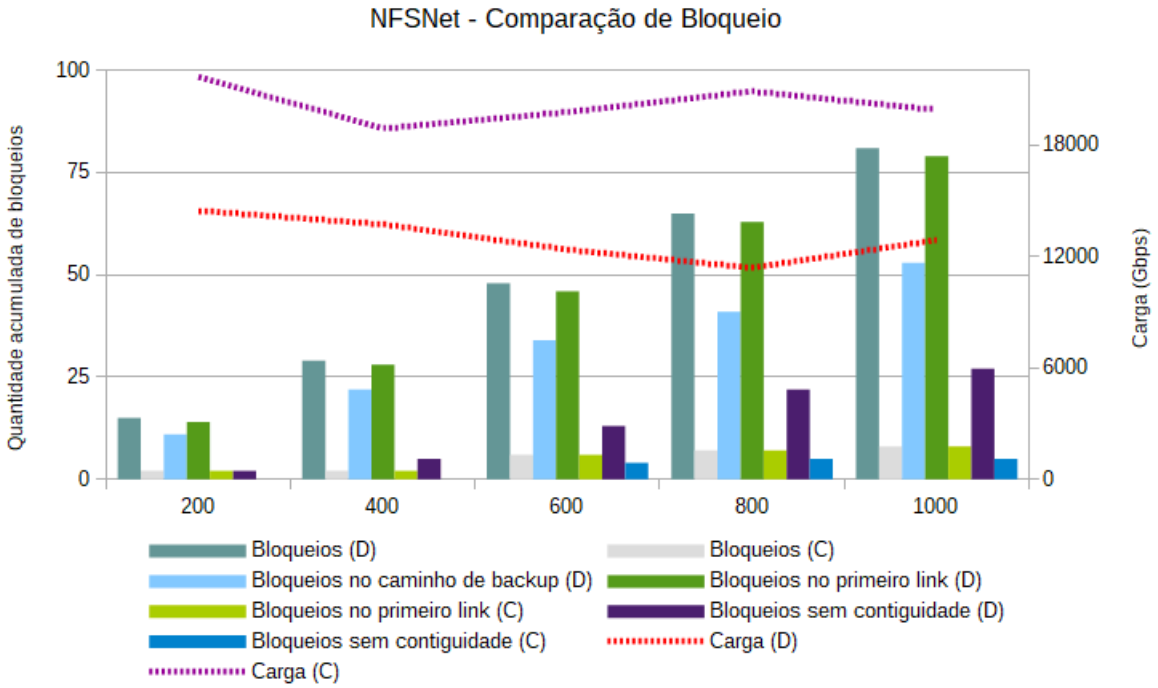

Figura 8.9 – NFS Net - Comparativo de Carga e Bloqueio

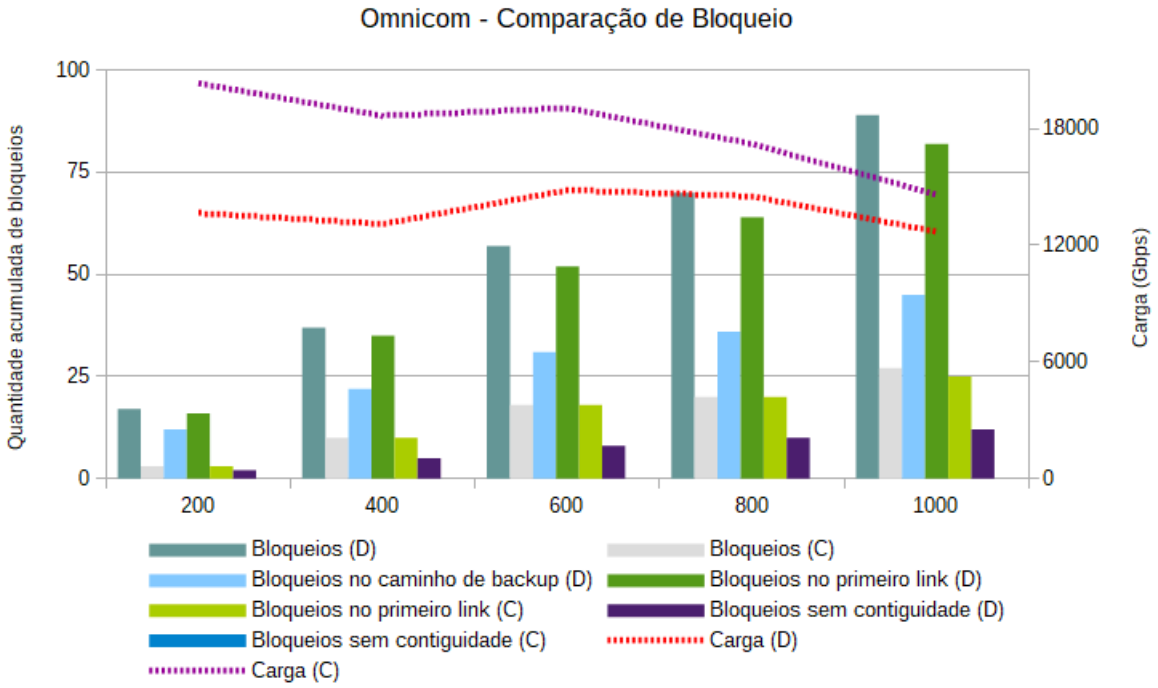

Figura 8.10 – Omincom - Comparativo de Carga e Bloqueio

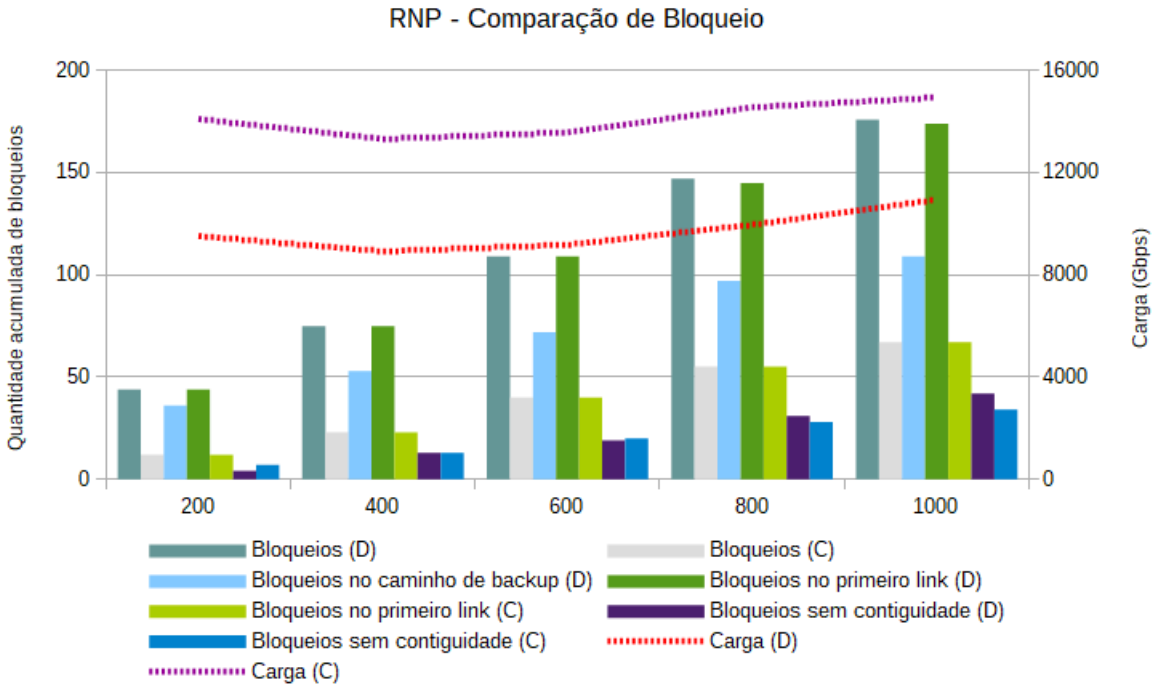

Figura 8.11 – RNP - Comparativo de Carga e Bloqueio

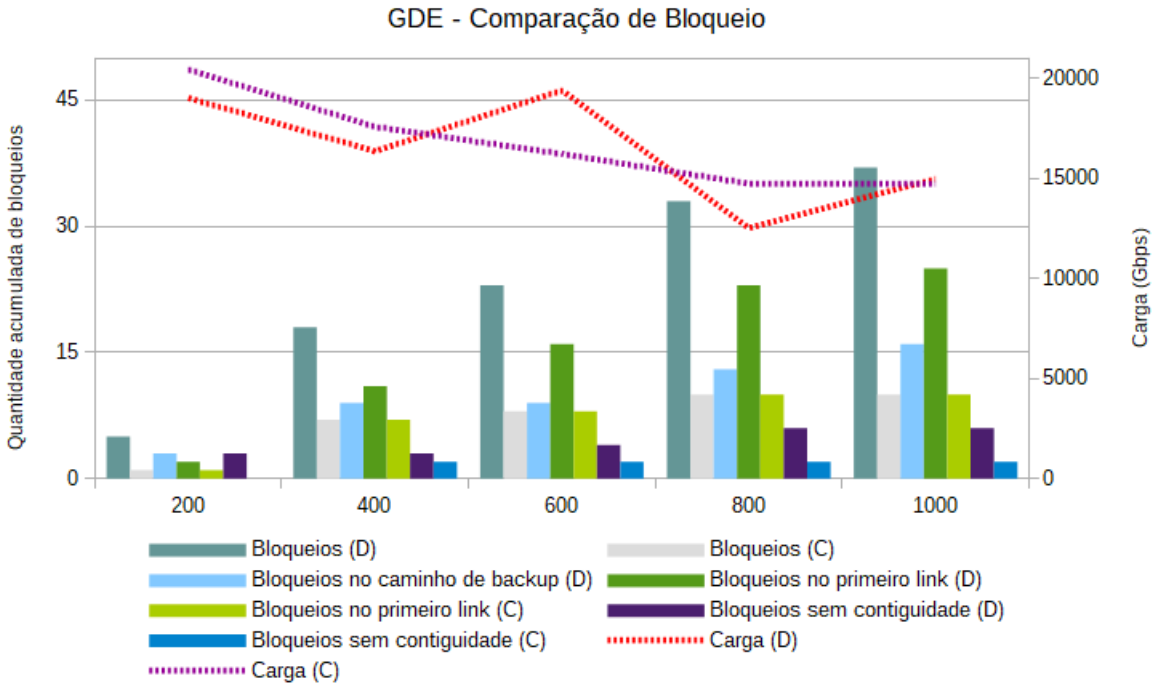

Figura 8.12 – GDE - Comparativo de Carga e Bloqueio

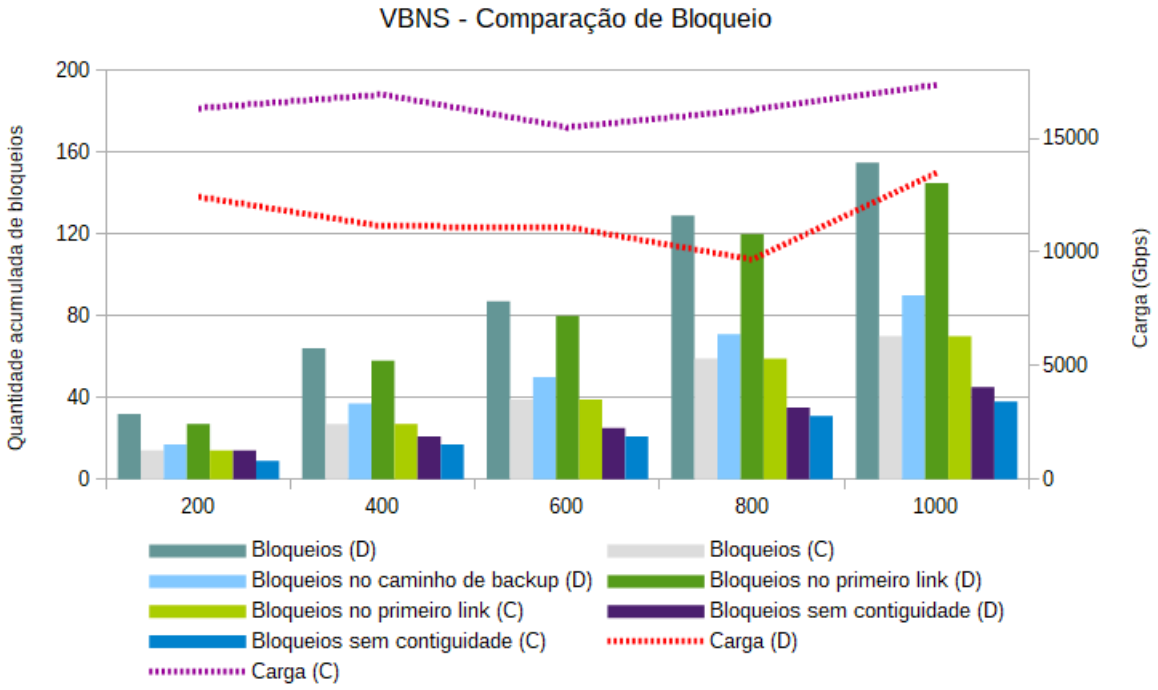

Figura 8.13 – VBNS - Comparativo de Carga e Bloqueio

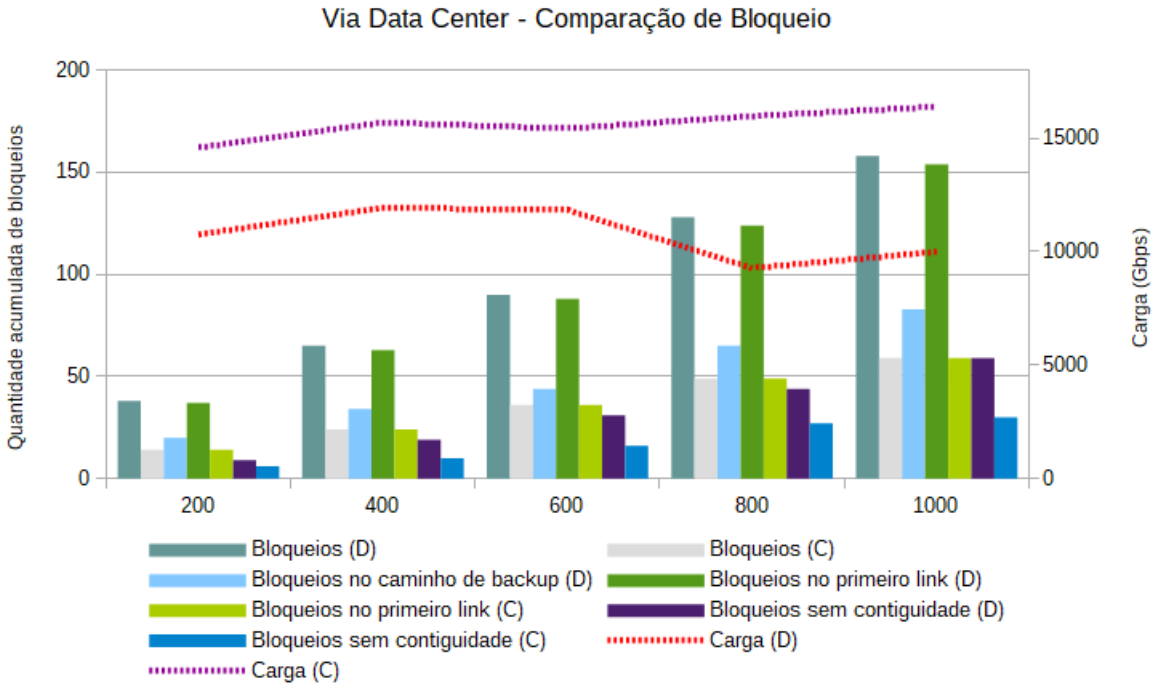

Figura 8.14 – Via Data Center - Comparativo de Carga e Bloqueio

Tabela 8.3 – Comparação Detalhada do Bloqueio por Rede e Tipo de Proteção

Rede	**BD**	**BC**	**TD**	**TC**	**RCD**
Arnes	198	107	19,80	10,70	54,04
Cox	62	24	6,20	2,40	38,71
Deutsch	67	29	6,70	2,90	43,28
2 USA	195	68	19,50	6,80	34,87
Memorex	229	87	22,90	8,70	37,99
Metrona	193	84	19,30	8,40	43,52
NFSNet	81	8	8,10	0,80	9,88
Omnicom	89	27	8,90	2,70	30,34
RNP	176	67	17,60	6,70	38,07
GDE	37	10	3,70	1,00	27,03
VBNS	155	70	15,50	7,00	45,16
Via Data Center	158	59	15,80	5,90	37,34

Significado das Abreviações	
BD	Bloqueios com proteção dedicada
BC	Bloqueios com proteção compartilhada
TD	Taxa de bloqueio com proteção dedicada %
TC	Taxa de bloqueio com proteção compartilhada %
RCD	Razão entre taxa de bloqueios com proteção compartilhada e dedicada %

8.2 Utilização de Recursos

Em nossas simulações, também registramos o percentual de utilização dos recursos da rede e, deste percentual, a razão entre a quantidade alocada para proteção e para trabalho.

O gráfico da figura 8.15 mostra um comparativo percentual da quantidade de recursos utilizados para proteção e trabalho em cada uma das redes.

Percebemos que a quantidade de recursos alocados para proteção compartilhada foi maior do que a esperada, não se revelando uma grande economia em termos diretos. Em todas as redes, a razão de recursos entre proteção compartilhada e proteção dedicada ficou em torno de 0,9. Porém, em termos de impacto no bloqueio, essa diferença se revelou grande, em alguns casos fazendo com que a taxa de bloqueio com proteção compartilhada ficasse em 9% da taxa obtida com proteção dedicada. Esta melhora considerável na taxa de bloqueio é explicada pela diferença da fragmentação da rede (menor fragmentação com o uso de proteção compartilhada), conforme mostra o gráfico da figura 8.16.

A fragmentação da rede foi calculada com uma equação simplificada da proposta de (SINGH; JUKAN, 2017), a partir da razão entre o somatório das demandas aceitas na condição fragmentada e o somatório da quantidade de demandas idealmente aceitas, se todo o espaço livre do $link$ fosse contíguo. Também incluímos outra variante na equação ao considerarmos somente o espectro a partir do primeiro *slot* comprometido para proteção, uma vez que a política de atribuição adotada foi a $FirstLastFit$ e desejamos obter apenas a fragmentação do espectro de proteção. A equação 8.1 mostra como a métrica foi avaliada.

$$F_l = 1 - \frac{\sum_{i=1}^{I} \sum_{j=1}^{J} j}{\sum_{k=1}^{K} k} \tag{8.1}$$

Onde:

- F_l: Fragmentação do link l;
- i: Índice do i-ésimo bloco livre;
- I: Total de blocos livres;
- j: Índice do j-ésimo *slot* livre no bloco i;
- J: Total de *slots* livres em cada bloco i;
- k: k-ésimo *slot* livre no bloco ideal;
- K: Total de *slots* livres;

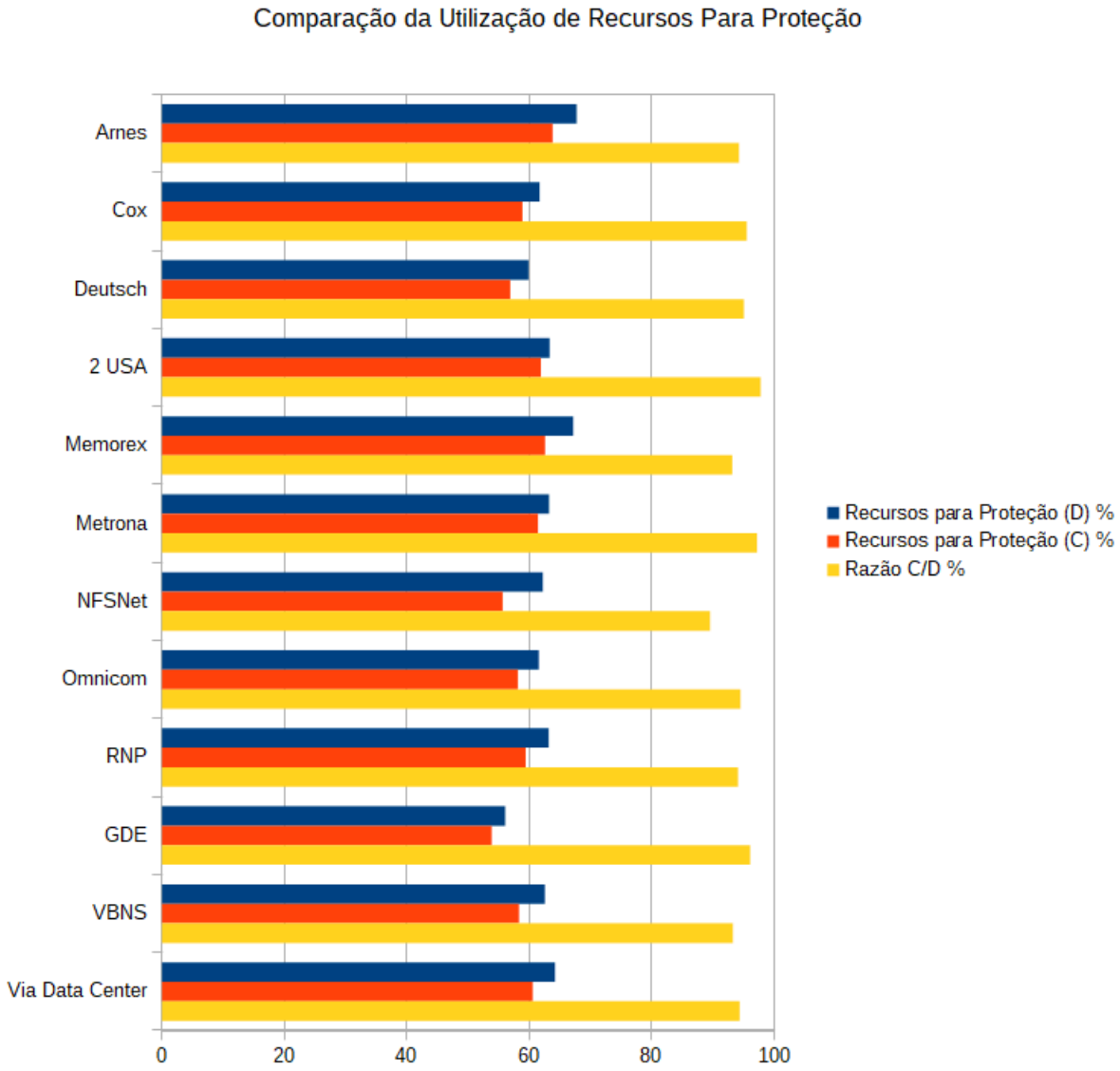

Figura 8.15 – Comparativo da Utilização de Recursos por Proteção

8.3 Eficiência do Espectro Ótico

A eficiência do espectro depende diretamente do padrão das demandas de tráfego solicitadas para a rede. Isto significa que o espectro sobrealocado (pela granularidade do *slot*) irá variar apenas em quantidade absoluta, devido ao número de requisições, mas a quantidade relativa sempre será a mesma para cada taxa de serviço. Ou seja, uma demanda de 40 Gbps, com modulação 8-QAM irá sempre ocasionar um desperdício de mais de 90% de um *slot*, pois um único *slot* permite uma taxa de 37,5 Gbps, sendo necessária a utilização de mais um *slot* para o restante (2,5 Gbps).

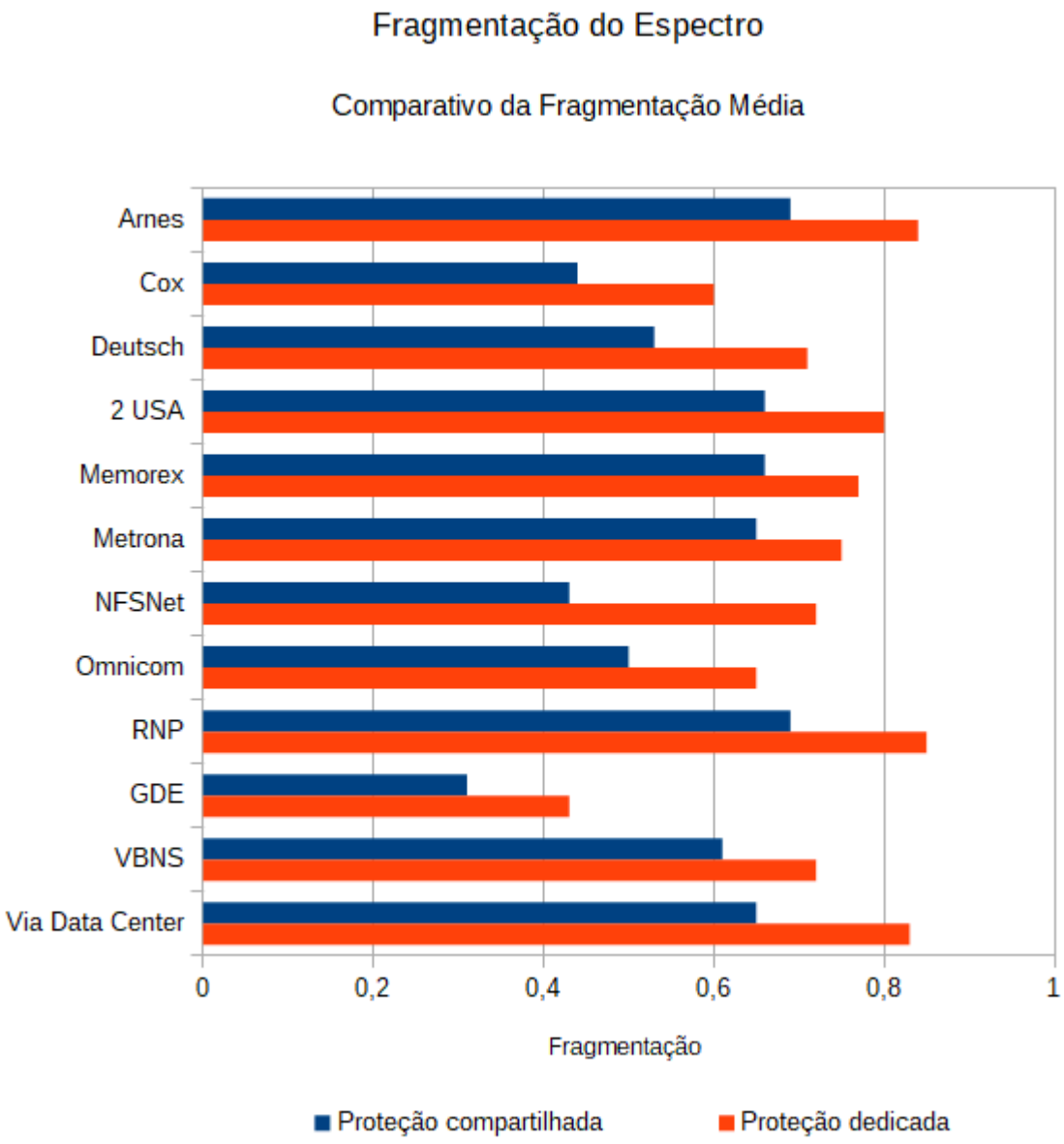

Figura 8.16 – Fragmentação

Por outro lado, uma demanda de 100 Gbps, requer 3 *slots* e ocasiona apenas 33% de desperdício em um *slot*, uma vez que dois *slots* suportam 75 Gbps de tráfego e o terceiro proverá os 25 restantes, desperdiçando uma capacidade de 12,5 Gbps.

Em nossa simulação, executamos requisições de 40, 100, 200 e 400 Gbps e 1 Tbps, distribuídas conforme a lista 8 e a partir disso já temos um quadro de eficiência espectral previsto, pois fixamos a quantidade de 1000 requisições por simulação. Como a distribuição não é um parâmetro exato, precisamos contar quantas requisições solicitaram cada taxa.

O gráfico da figura 8.1 e a tabela 8.3 detalham mais essas informações.

Tabela 8.4 – Eficiência Espectral Por Taxa de Serviço (Demanda em Gbps)

Taxa de Serviço (Gbps)	40	100	200	400	1000
Slots Necessários	2	3	6	11	27
Espectro Comprometido (GHz)	25	37,5	75	137,5	337,5
Espectro Ideal	13,33	33,33	66,67	133,33	333,33
Capacidade da Faixa Alocada (Gbps)	75	112,5	225	412,5	1012,5
Desperdício de Capacidade (Gbps)	35	12,5	25	12,5	12,5
Desperdício Relativo a 1 slot	0,933	0,333	0,667	0,333	0,333
Eficiência Espectral Unitária	0,533	0,889	0,889	0,970	0,988
Quantidade de Requisições	323	271	218	116	72
Eficiência Espectral Ponderada	0,172	0,241	0,194	0,112	0,071
Eficiência Espectral Média da Simulação			0,791		

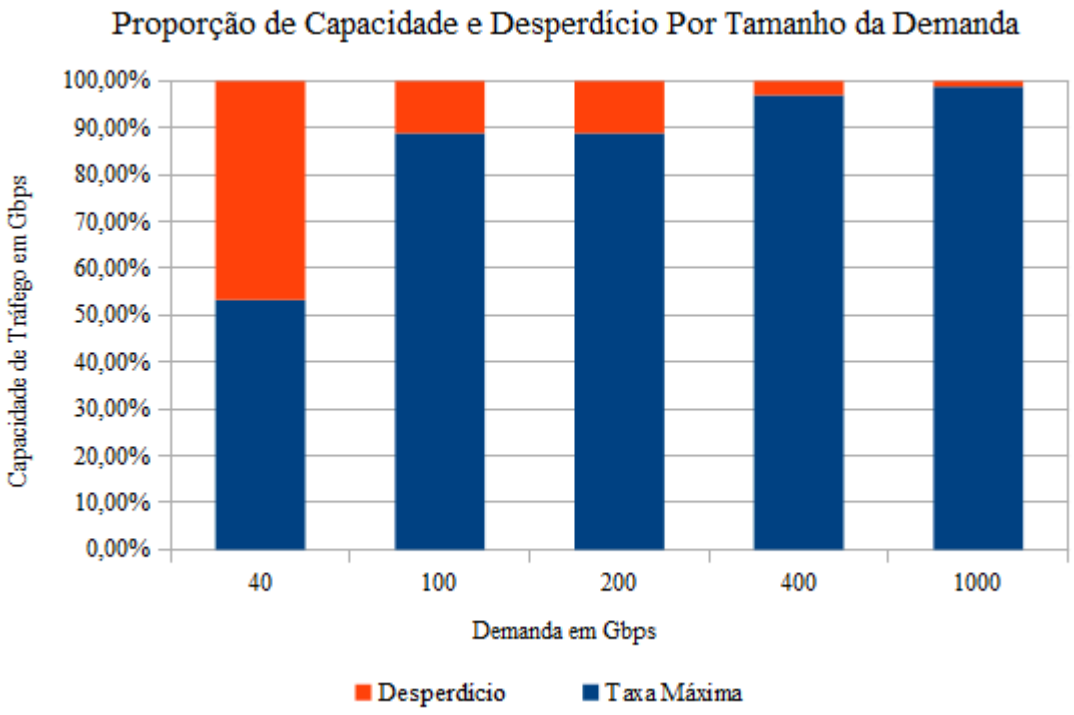

Figura 8.17 – Proporção da Capacidade e Desperdício por Tamanho de Demanda

9 CONSIDERAÇÕES FINAIS

A partir dos resultados obtidos e aqui apresentados, e embasados nos estudos prévios e ainda pelo que era esperado, pudemos constatar que a estratégia de proteção tem impacto significativo na performance da rede, podendo afetar e até comprometer a disponibilidade de serviço.

A proteção dedicada sempre compromete uma quantidade grande de recursos em relação a quantidade necessária para os caminhos de trabalho. Assim, não se tem uma boa eficiência de utilização total de recursos, pois o caminho de proteção é pelo menos tão custoso quanto o caminho de trabalho e geralmente é mais. Diante disso, uma razão próxima a 1 entre quantidade de recursos comprometidos para proteção e quantidade comprometida para trabalho é uma situação bem favorável.

Já na proteção compartilhada, essa eficiência pode ser aumentada, conforme mostrado no gráfico 8.15.

Nos exemplos de rede utilizados em nossas simulações, de forma geral, a quantidade de recursos comprometidos pela proteção compartilhada em relação a proteção dedicada, ainda pode ser considerada alta, pelas características topológicas das redes. Acreditamos que as redes tipo $core$, que geralmente têm baixo grau nodal ocasionam esta situação.

Cabe dizer, a partir disso, que um bom projeto de rede deve dimensionar a necessidade de recursos tentando criar um equilíbrio entre proteção e disponibilidade. Em situações específicas, onde seja necessário o uso de proteção dedicada completa, a rede deverá ser sobredimensionada.

A proteção compartilhada se mostra ideal para cenários onde ocorrem poucas falhas ou a sua recuperação é rápida. Uma alternativa seria utilizar soluções híbridas, protegendo rotas mais críticas de forma dedicada e as demais de maneira compartilhada.

Ainda, devemos considerar que o estudo aqui apresentado se refere a um pequeno conjunto de aspectos afetados pela proteção e que envolvem todo o problema do RMLSA nas redes elásticas. É possível evoluir este estudo para considerar outras características das redes, tais como probabilidade de falhas, distância física entre os nós etc... para realizar uma simulação mais fiel à realidade das mesmas.

REFERÊNCIAS

CANDIA, M. P. d. L. **Heurística Para Alocação de Espectro em Redes Ópticas Elásticas Baseada em Medidas de Fragmentação**. 2014. Dissertação (Mestrado em Ciência da Computação) — INPE - Instituto Nacional de Pesquisas Espaciais.

EIRA, A. et al. Multi-objective Design of Survivable Flexible-Grid DWDM Networks. **OSA Publishing**, [S.l.], 2014.

ELLINAS, G. et al. Practical Issues for the Implementation of Survivability and Recovery Techniques in Optical Networks. **Research Gate**, [S.l.], 2016.

KLINKOWSKI, M. et al. Elastic Spectrum Allocation for Time-Varying Traffic in FlexGrid Optical Networks. **IEEE - Journal on Selected Areas in Communications, V.31, Issue 1**, [S.l.], 2013.

MARINO, P. P.; DELGADO, M. V. B.; ZARAGOZA, J. L. I. Evaluating Internal Blocking in Noncontentionless flexi-grid ROADMs. **Journal of Optical Communications and Networking**, [S.l.], 2015.

MORAIS, R. Desenho Topológico de Redes Ópticas. **Universidade de Aveiro**, [S.l.], 2008.

MOURA, P. M.; DRUMMOND, A. C. **FlexGridSim**: flexible grid optical network simulator. 2018.

ROSA, A. N. F. et al. Statistical analysis of blocking probability and fragmentation based on Markov modeling of elastic spectrum allocation on fiber link. **Optics Communications**, [S.l.], v.354, p.362–373, 2015. QC 20151016.

SATKUNARAJAH, S.; KRISHANTHMOHAN, R.; RAGEL, R. G. Pre-configured Backup Protection With Limited Resource Sharing in Elastic Optical Networks. **IIIE - International Conference on Industrial and Information Systems**, [S.l.], 2015.

SHEN, G.; GUO, H.; BOSE, S. K. Survivable elastic optical networks: survey and perspective. **Springer**, [S.l.], 2016.

SINGH, S. K.; JUKAN, A. Efficient Spectrum Defragmentation with Holding-time Awareness in Elastic Optical Networks. **IEEE/OSA Journal of Optical Communications and Networking**, [S.l.], v.9, 2017.

TESSINARI, R. S. **A Fairness-Focused Spectrum Assignment Algorithm For Elastic Optical Networks**. 2016. Tese (Doutorado em Ciência da Computação) — Universidade Federal do Espírito Santo - UFES.

TESSINARI, R. S. et al. ElasticO++: an elastic optical network simulation framework for omnet++. **Optical Switching and Networking, Vol 22**, [S.l.], 2016.

VELASCO, L. et al. On the Performance of Flexgrid-Based Optical Networks. **OCDN)**, [S.l.], 2012.

YUAN, S.; JUE, J. Shared Protection Routing Algorithm for Optical Network. **Department of Computer Science, University of Texas at Dallas Richardson, TX 75083**, [S.l.], 2003.